Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs

Problem Formulation and Solution Strategy

Lynne Genik
DRDC Centre for Security Science

Paul Chouinard
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Canada

Principal Author

Original signed by Lynne Genik

Lynne Genik, MSc

DRDC Centre for Security Science

Approved by

Original signed by Andrew Vallerand

Dr. Andrew Vallerand

DRDC Centre for Security Science

Approved for release by

Original signed by Dr. Mark Williamson

Dr. Mark Williamson

DRDC Centre for Security Science

Abstract

This paper presents the problem formulation and solution strategy component of the EMBC-DRDC collaborative project agreement for improving EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Assurance Programs. The methodology is described; the NATO Code of Best Practice for C2 Assessment and a soft operations research approach were applied, along with aspects of capability based planning, systems engineering, and risk management. Preliminary literature searches were performed and are documented here. Stakeholder groups are described and the questions used to elicit their perspectives on the programs and related issues are presented. The result of the analysis was the identification of program requirements, gaps, and proposed projects by DRDC to address aspects of the gaps. The proposed projects include adapting the Major Events Security Framework for use by EMBC, CI assessment tool development through pilot projects, and contracts for a community resilience framework and scenario mission to task templates, among several others.

Résumé

Le présent rapport explique les stratégies de formulation et de résolution du problème du projet collaboratif de RDDC et d'EMBC visant à améliorer les programmes d'analyse des dangers, des risques et de la vulnérabilité (ADRV) et d'infrastructures essentielles (IE). On y décrit la méthodologie employée, qui se résume à ceci : utilisation d'une approche de recherche opérationnelle souple et application des principes du Code des pratiques exemplaires d'évaluation du C2 de l'OTAN à divers aspects de la planification axée sur les capacités, à l'ingénierie des systèmes et à la gestion des risques. Les recherches documentaires préliminaires sont aussi décrites dans le présent rapport. On y présente les groupes d'intervenants consultés et les questions qui leur ont été posées afin de recueillir leurs points de vue au sujet des programmes à l'étude et des problèmes connexes. L'analyse a permis de cerner les besoins et les lacunes des programmes et de proposer des projets de RDDC en vue de combler les lacunes en question. Parmi ces propositions, on trouve notamment l'adaptation du Cadre de sécurité des grands événements pour les besoins d'EMBC, le développement d'un outil d'évaluation des infrastructures essentielles dans le cadre de divers projets pilotes, et l'octroi de contrats pour l'établissement d'un cadre de résilience communautaire et l'élaboration de modèles de synthèse mission-tâches.

Executive summary

DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs:

Lynne Genik, Paul Chouinard, DRDC Centre for Security Science; DRDC CSS TM 2012-015; Defence R&D Canada – CSS; October 2012.

Background: EMBC and DRDC established a collaborative project following the Vancouver 2010 Olympic and Paralympic Winter Games with the objective of demonstrating the value of an operations research and analysis approach to improving emergency management capabilities. The areas of focus are EMBC's Hazard Risk Vulnerability Analysis (HRVA) Program and Critical Infrastructure Assurance Program (CIAP). This paper presents the problem formulation methodology and solution strategy for the first phase of the project.

Method: The problems to be tackled with the HRVA program – "taking it to the next level" - and the CIAP – "enhancing CI resilience" - fall under the category of wicked problems given their multi-agency dimensions and somewhat vague objectives; hence, a soft operations research approach was applied. The NATO Code of Best Practice was used as a foundation, applying relevant aspects of capability based planning, systems engineering, and risk management. Literature reviews on risk management/assessment and critical infrastructure were performed, including a review of international standards, national approaches, and academic and practitioner literature. Stakeholder groups were consulted for their perspectives.

Results: A requirements and gaps analysis of each program was provided to EMBC, along with the proposal of a number of DRDC projects to close gaps. The high-level categories of gaps are summarized in this paper, but the specific details of the requirements and gaps are not. The DRDC project proposals are described along with the extent to which they address the categories of gaps. In total eleven proposals were presented to and evaluated with EMBC.

Significance: These wicked problems are complex, unique problems and there is no "one, correct" solution. Addressing the problems involves understanding the perspectives of multiple stakeholders and finding common ground. The goals of this work include shared awareness and understanding among the emergency management (EM), CI, and research communities and contributions that allow for improvements to the four pillars of the EM cycle, that is, mitigation/prevention, preparedness, response, and recovery, for HRVA and CI, not only in BC but nationally.

Future plans: At present, nine DRDC projects are being pursued, including: CI assessment tool development (includes several project proposals), adaptation of the Major Events Security Framework, contracts for a community resilience framework and scenario mission to task templates, extensive literature searches, and research on multi-agency collaboration. As the projects progress it is anticipated that an enhanced problem understanding and way forward will develop among stakeholders.

Sommaire

Soutien offert par RDDC aux programmes d'analyse des dangers, des risques et de la vulnérabilité (ADRV) et d'infrastructures essentielles (IE) d'Emergency Management British Columbia (EMBC)

Lynne Genik, Paul Chouinard, RDDC – Centre des sciences pour la sécurité; DRDC CSS TM 2012-015; R & D pour la défense Canada – CSS; octobre 2012.

Contexte : À la suite des Jeux olympiques et paralympiques d'hiver de Vancouver en 2010, EMBC et RDDC ont lancé un projet collaboratif dans le but de démontrer l'utilité de l'analyse et de la recherche opérationnelles lorsqu'il s'agit d'améliorer des capacités de gestion des urgences. Les sujets à l'étude sont le Programme d'analyse des dangers, des risques et de la vulnérabilité (ADRV) et le Programme de fiabilité des infrastructures essentielles (PFIE) de l'EMBC. Le présent rapport décrit la méthode de préparation de l'énoncé du problème et la stratégie utilisée pour résoudre le problème durant la première phase du projet.

Méthode : Les problèmes à aborder (« passer à l'étape suivante », pour le programme ARDV, et « accroître la résilience des infrastructures essentielles », pour le PFIE) sont classés dans la catégorie des problèmes épineux, étant donné qu'ils concernent de multiples organisations et que leurs objectifs sont plutôt vagues. Par conséquent, il a fallu opter pour une méthode de recherche souple. Comme point de départ, nous avons utilisé le Code des pratiques exemplaires de l'OTAN duquel nous avons tiré les principes pertinents de planification axée sur les capacités, d'ingénierie des systèmes et de gestion des risques. Nous avons consulté différents ouvrages portant sur la gestion et l'évaluation des risques et sur les infrastructures essentielles, notamment sur les normes internationales et les méthodes utilisées dans différents pays, ainsi que des ouvrages d'universitaires et de spécialistes. Différents groupes d'intervenants ont également été consultés afin de connaître leurs points de vue.

Résultats : Nous avons présenté à EMBC une analyse des besoins et des lacunes de chacun des programmes à l'étude en plus de lui proposer différents projets de RDDC pour combler les lacunes en question. Un résumé des principales catégories de lacunes est présenté dans le rapport; cependant, les détails précis des besoins et des lacunes ne sont pas fournis. Une description des projets de RDDC proposés est offerte et nous indiquons dans quelle mesure chacun d'eux peut contribuer à la résolution des problèmes cernés. Au total, onze projets ont été proposés à EMBC et évalués avec l'aide de cette dernière.

Portée : Les problèmes étudiés dans le cadre de cette étude sont des problèmes épineux, complexes et uniques pour lesquels il n'existe pas de solution parfaite. Pour résoudre ces problèmes, il faut recueillir et chercher à réconcilier les points de vue de différents intervenants afin de trouver la solution la plus satisfaisante possible. Cette étude a notamment pour but d'établir des bases communes de connaissances entre les spécialistes de la gestion des urgences, des infrastructures essentielles et de la recherche et de réaliser des travaux qui contribueront au renforcement des quatre piliers du cycle de gestion des urgences – c'est-à-dire l'atténuation et la prévention, la préparation, l'intervention et le rétablissement – dans le but d'améliorer les programmes d'ARDV et de protection des infrastructures essentielles non seulement en Colombie-Britannique, mais partout au pays.

Recherches futures : À l'heure actuelle, neuf projets de RDDC sont en cours, dont les suivants : le développement d'un outil d'évaluation des infrastructures essentielles (comprends plusieurs propositions de projet), l'adaptation du Cadre de sécurité des grands événements, l'octroi de contrats pour l'établissement d'un cadre de résilience communautaire et l'élaboration de modèles de synthèse mission-tâches, des recherches documentaires approfondies, et une recherche sur la collaboration multiorganisationnelle. Ces projets devraient aider petit à petit les différentes parties concernées à connaître de mieux en mieux le problème et à planifier les prochaines étapes .

Table of contents

List of figures

List of tables

Acknowledgements

We would like to acknowledge our partners at Emergency Management British Columbia, particularly Heather Lyle, Director of Integrated Public Safety (IPS), and former IPS Research and Project Coordinator, Miranda Myles.

1 Introduction

1.1 Background

DRDC provided scientific support and advice to Emergency Management British Columbia (EMBC) and the Royal Canadian Mounted Police (RCMP)-led Integrated Security Unit (ISU) for the Vancouver 2010 Olympic and Paralympic Winter Games (V2010) as part of the Major Events Coordinated Security Solutions (MECSS) project. From 2008-2010, the first author was an embedded scientific advisor with EMBC's Integrated Public Safety (IPS) in British Columbia (BC) and the second author provided scientific support for the V2010 critical infrastructure (CI) project as the MECSS CI domain lead.

Through the MECSS project, DRDC was tasked with supporting the ISU for "the CI problem", and performed an analysis to provide an objective, scientific basis for the ISU to set priorities for CI liaison, planning and preparations. The analysis facilitated discussions on coordination between the ISU and key asset owners, shifted the focus from "boots on the ground" protection to a coordinated response, increased the confidence of the ISU with respect to the CI problem, and separated ISU CI issues from broader regional issues. In the final months approaching the Games, an analysis was undertaken for IPS with the objective of identifying the most critical CI service dependencies for the Emergency Management Response System (EMRS) for the remaining time period up to and including the Games. The results of the analysis were used by the first author to lead CI outreach to asset owners on behalf of EMBC.

Numerous challenges became apparent during the course of the CI work for V2010. Initially, IPS and the ISU were working together on the CI problem, and IPS led the collection of data from more than 125 assets owners with an EMBC-developed CI rating workbook. However, information sharing between the ISU and IPS became complicated by a V2010 confidentiality/non-disclosure agreement (NDA) for CI data (demanded by many assets owners) between CI asset owners and the ISU. The NDA prevented EMBC from having access to the CI data and analysis results due to security classifications imposed by the NDA and the lack of classified information handling capabilities at the provincial level. During the analysis of the data submitted using EMBC's CI rating workbook, DRDC identified problems with the assessment methodology/tool and shared these with EMBC; however, DRDC had neither the mandate nor opportunity at that time to assist EMBC in addressing the problems. In addition, the data could not be shared to provide concrete examples of the problems and following the games, as per the NDA, the data was destroyed.

With the conclusion of V2010, EMBC and DRDC expressed interest in a continued partnership. After discussions on mutual areas of interest, a DRDC-EMBC project plan [1] was proposed, which was ultimately blessed by DRDC, EMBC, and Public Safety Canada (PSC)[1]. The EMBC-DRDC collaborative project objectives are to:

[1] Note that PSC has the federal mandate of working directly with the provinces

- "Evaluate options for a science and technology (S&T)-informed, structured approach to enhance BC emergency management capabilities at the provincial, regional and municipal levels.

- Demonstrate the value of S&T-informed, structured approaches for BC emergency management.

- Identify recommendations for further use of S&T-informed, structured approaches to enhance BC emergency management capabilities and for extending the results nationally." [1]

Therefore, the intent is to bring value to EMBC programs and capabilities through applying a scientific (that is, operational research and analysis (OR&A)) approach. This was a novel project agreement for DRDC, enabling DRDC CSS' mission "to strengthen Canada's ability to prevent, prepare for, respond to, and recover from acts of terrorism, crime, natural disasters, and serious accidents through the convergence of science and technology with policy, operations and intelligence"[2], with the intent that the approaches, methodologies, tools, etc. developed through the project be made available to other provinces and nationally.

1.2 Purpose

The purpose of this report is to document the authors' work for the first phase of the DRDC-EMBC project, namely in the problem formulation and solution strategy. The initial phase of the project included an assessment of the requirements for EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) programs, comparing the requirements with existing initiatives to identify gaps, and proposing DRDC projects to support EMBC in making improvements to their programs.

1.3 Scope

1.3.1 Project Scope

The collaborative project focuses primarily on two areas of work:

1. Hazard Risk Vulnerability Analysis (HRVA);

2. Critical Infrastructure (CI);

and a third area in support of the above capabilities:

3. Intelligence and information sharing.

CI was an obvious area of collaboration given the expertise developed by DRDC during the CI work for V2010 and the problems identified during V2010. HRVA was identified by EMBC as a priority area going forward from the games and it was agreed that it was amenable to an OR

[2] DRDC CSS web site http://www.css.drdc-rddc.gc.ca/index-eng.asp

approach. Finally, EMBC experienced a number of challenges related to intelligence and information sharing during V2010 for CI and other domains. This was highlighted by the first author during command and control analysis of the South West Provincial Regional Emergency Operations Centre during V2010 preparatory exercises and the Games [2].

Emergency management (EM) is commonly discussed in terms of the four pillars of the emergency management cycle as illustrated in the figure below.

Figure 1: The Emergency Management Cycle[3]

The pillars can be described as follows [3]:

- Mitigation and prevention involves reducing or eliminating hazards/threats and their impacts. Examples of mitigation and prevention measures are land-use planning and public education;

- Preparedness involves measures to ensure that individuals and organizations are prepared to react. Examples are emergency plans, mutual aid agreements, resource inventories, training, exercises, and emergency communications systems.

- Response involves activities that deal with an incident to manage and limit the impacts (such as loss of life, injury, economic and environmental impacts, etc.) of the incident. Examples of response measures are creating and maintaining situational awareness, prioritizing actions, allocating resources, ensuring continuity of services and restoring critical infrastructure;

- Recovery involves restoring the community. Examples of recovery measures include providing shelter and financial assistance, managing donations, rebuilding, etc.

[3] From http://www.tularehhsa.org/index.cfm/office-of-emergency-services/what-is-oes/

When considering risk management and critical infrastructure, one must consider all aspects of the EM cycle. For example, risk assessment involves the identification of hazards and threats, which can then lead to the mitigation and prevention of these hazards and threats based on priority, resources, risk tolerance, etc. Organizations commonly implement preparedness and response measures based on risk analysis and evaluations, and recovery priorities can also be viewed in terms of risk.

1.3.2 Document Scope

As mentioned, this report documents the problem formulation and solution strategy for the DRDC-EMBC project. However, due to the sensitivity of the some information, such as the requirements and gaps analyses of the BC programs, results are presented in general terms in this document.

The literature reviews for risk management and CI are preliminary and used to evaluate the BC programs against best practices (if they exist). More in-depth literature reviews are recommended. In particular, at this stage, other national approaches were examined only to identify tools or processes that might be of use for BC. There was no intention for a formal examination of the full processes used by other nations. Such an analysis would need to take into consideration a national assessment of the differences between Canada and other nations. While this might be a valuable national exercise it was deemed beyond the scope and resources of examining two programs within a single Canadian province.

1.4 Document Structure

The next chapter discusses the methodologies applied to the problem formulation, including the NATO Code of Best Practice for C2 Assessment, capability based planning, wicked problems and soft operations research. Chapter 3 is specific to risk assessment and chapter 4 to critical infrastructure, each containing a literature review followed by information related to DRDC's analysis of EMBC's respective programs. Proposed solutions/projects are presented in chapter 5 along with an evaluation of the solutions. Finally, a summary is provided in chapter 6.

2 Methodology

2.1 NATO Code of Best Practice for C2 Assessment

EMBC identified two priority areas for the collaborative work with DRDC. One was their Hazard, Risk and Vulnerability Assessment (HRVA) program and the other was their Critical Infrastructure Assurance Program (CIAP). Both priority areas shared a couple of key characteristics that allowed an overall common approach to be used. These were:

- Ambiguous objectives. The objective for the HRVA program was more of an aspiration (that is, "taking it to the next level") for improving and building on the currently successful program than a clear goal. The aim of the CIAP was "enhanced CI resilience", which was not much clearer. The EMBC objectives for both programs could be seen more as acknowledgement that these were areas for improvement but that more work was required to identify what improvements were needed; and

- Multi-agency decision-making processes to treat risk. Both programs deal with risk management (that is, the need to identify risk, assess risk and develop strategies to reduce risk) across a community of stakeholders. There are well known methods for risk management for implementation by an organization. However, implementing these methods in a multi-agency context is a challenging management problem.

The foundation for the DRDC approach was the NATO Code of Best Practice for C2 (Command and Control) Assessment [4]. This was developed by the military operational research and analysis community following the end of the Cold War. NATO's operations had shifted from traditional, military-led war-fighting to other types of operations, such as humanitarian aid, disaster relief, emergency evacuations, peacekeeping, etc. for which the military was often in a supporting role for a civilian led mission. The changed nature of operations also meant that physical systems were less important than those related to command and control (C2) problems dominated by informational, behavioural and cognitive issues. This change forced the operational research and analysis (OR&A) community to reassess their traditional analytical approaches. The result was the Code of Best Practice that built on best practices from the past while providing recommendations for analyzing the multi-dimensional, complex management issues that characterize current operations involving military forces. Since the publication of the Code of Best Practice it has become a standard reference for the OR&A community and has been successfully applied to many types of complex management problems beyond those involving military forces.

The Code of Best Practice recommends the following steps for analysis of complex management problems:

1. Preparing for Success: The initial step of the process is to develop a common understanding of the study's goals, objectives, scope, stakeholders, etc. and to build an assessment team with the requisite skills and experience.

2. Problem Formulation: As stated by the Code, "effective problem formulation is fundamental to the success of all assessments, but particularly in C2 assessment because issues are often ill-defined and complex, involving many dimensions and a rich context."

3. Solution Strategies: The problem formulation defines "what" will be addressed or achieved. The solution strategy articulates "how". The strategy must balance what is desirable with the practicalities of what is achievable.

4. Measures of Merit: Measures of merit provide the basis for comparing decision options and the set of measures must be broad enough to encompass all of the critical dimensions and issues associated with the problem.

5. Human and Organizational Factors: As noted above the Code was developed due to the shift in traditional operational research and analysis from predominantly assessing physical systems to one where assessing the human and organizational dimension is critical. A successful study requires identifying the key human and organizational factors that affect the problem.

6. Scenarios: Context is critical to the understanding and assessment of complex operations. Developing a set of scenarios provides a means of explicitly capturing the key assumptions associated with the context of the problem.

7. Methods and Tools: The OR&A community typically uses a wide variety of tools for assessing problems. The choice of methods and tools must be tailored to the problem. Criteria for model and tool selection include functionality (that is, the model or tool adequately addresses the problem's issues) and performance (that is, the model is practical).

8. Data: Data is central to good assessments and the Code makes several recommendations with respect to data collection and management.

9. Risk and Uncertainty: Risk and uncertainty are inherent in any study, but the nature of complex operations requires the analyst to be "alert to the possibility of chaotic behaviours arising from dynamic interactions of human and organizational factors". The Code provides guidance on the proper treatment of risk and uncertainty in the study.

10. Products: There are several products associated with a proper OR&A study that include the study plan, status reports, project journal and final report/briefing. Importantly, the final report should be understandable to the client who should also be able to brief the results on their own.

As noted above, the objectives of EMBC for both the HRVA program and CIAP were somewhat ambiguous. This meant that the "problem formulation" step recommended by the Code was not only important but likely to dominate the study. It could even be argued that a successful problem formulation was the objective of the EMBC-DRDC study. Therefore, it's worth noting that the Code states that problem formulation is an iterative process that is fundamentally a social process to develop a shared understanding of the problem amongst the EMBC client, EMBC's stakeholders and the DRDC study team. The assessment team should identify, develop and apply appropriate tools to support problem formulation. Potential tools include techniques for expert

elicitation, influence diagrams, casual maps, system dynamics models and other soft operations research techniques. This report documents the initial iteration of the problem formulation process. A follow-on phase of the project will deal with several proposed DRDC initiatives that are designed to enhance the shared understanding of the problem by EMBC and its stakeholder communities.

2.2 Capability Based Planning

There are a number of different approaches to longer term planning as described in the NATO report on long term defence planning [5]. Among the various approaches, capability based planning (CBP) was selected as a complement to systems engineering because it extends systems engineering principles to include consideration of the need for common tools (for example, common language, taxonomies, processes, etc.) to aid the coordination of planning where several stakeholder groups are involved. CBP also includes assessing the adequacy of inputs to a capability (that is, resources such as people, processes and tools) in the context of best value for cost (that is, cost-benefit analysis).

The formal capability based planning process defines a capability as having the ability to achieve a desired end, goal or objective under specified conditions [6]. Usually the ability is defined through a set of tasks that performed together achieve the desired end, goal or objective. CBP is a structured planning process that is intended to aid an organization in preparing for future challenges. Paul Davis, Rand Corporation, defined CBP as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern day challenges and circumstances while working within an economic framework that necessitates choice." [7]

The Technical Cooperation Program (TTCP), which includes scientists from the American, Australian, British, Canadian, and New Zealand military communities, developed a guide to CBP [8] that defined the general attributes of a good CBP process, which were:

- CBP is concept-led in that there is an overall stated purpose or goal for a capability;
- CBP is focussed on delivering outcomes;
- CBP uses good systems engineering principles, such as separating requirements from solutions;
- CBP uses scenarios to test the suitability of capabilities;
- CBP considers people, processes and their equipment when assessing the adequacy of current capabilities or proposed solutions to capability gaps; and
- CBP requires a common understanding amongst stakeholders.

The two EMBC programs of interest, the HRVA and CI Assurance programs can be seen as high level capability aspirations of the Province of BC. The former has the goal of aiding communities with reducing their risk from "all hazards" while the latter has the goal of "enhancing CI resilience".

The CBP framework can be applied to assess the adequacy of the two EMBC programs by asking appropriate questions that form part of a good CBP process. These questions include:

1. Is the overall goal clear enough to allow the development of a concept of how to achieve the goal?

2. Is the concept on how to achieve the goal adequate for identifying the required tasks and specified performance levels for those tasks to implement the concept?
3. Does the organization have adequate resources – people, processes, information and equipment – to carry out the required tasks to the specified performance levels?

Addressing these three questions for both EMBC programs provides a systematic method for identifying the requirements and gaps for each program. CBP is an iterative process; each iteration provides more specific answers progressively to the above three questions. For example, if the first iteration reveals inadequacies in the articulation of the programs goals, it will be challenging to completely articulate the required tasks and, therefore, nearly impossible to assess the adequacy of resources.

2.3 Wicked Problems and Soft Operations Research

One issue with CBP is that one of its supporting stanchions is systems analysis. A key underlying assumption of systems analysis is that it is possible to articulate goals and identify problems unequivocally. However, when dealing with political-social problems, articulating goals and defining the problem can be intractable. These types of problems were termed by Rittel and Weber "wicked" problems in their 1973 paper entitled, *Dilemmas in a General Theory of Planning* [9]. Rittel and Weber identified the following characteristics of wicked problems:

- There is no definitive formulation: To understand the problem depends on one's conception of the solution for the problem.
- There is no stopping rule: It's not clear when the problem is solved.
- Solutions to wicked problems are not true or false but good or bad: Solutions aren't distinguished by being a true or false solution but a good or bad or more likely as a better or worse solution. Often solutions will be selected because they are good enough.
- There is no immediate or ultimate test for the solution to a wicked problem: Solutions to wicked problems have waves of consequences. It may take some time to fully understand all the consequences. What was initially thought to be a good solution may eventually turn out bad and vice versa.
- Every solution is a one-shot event: There is no opportunity for trial and error. Solutions must be implemented to be understood, but implemented solutions have consequences that cannot be undone.
- Solutions to wicked problems are not enumerable or exhaustively describable: There is no way of knowing if all possible solutions have been found.
- Every wicked problem is essentially unique: Similarities to previous problems may be less important than the differences, which may mean that the solutions to the previous problems don't work for the problem at hand.

- Every wicked problem can be thought of as a symptom of another problem: The other higher level problem tends to be broader and more general and more difficult to solve. The level at which the problem solver stops cannot be decided on the basis of logic and is usually determined by the problem solver's self-confidence.

- The existence of a discrepancy explaining a wicked problem can be explained in numerous ways; and the choice determines the nature of the problem's resolution: The analyst or problem solver's world view is the strongest determinant in explaining a discrepancy.

- The planner has no right to be wrong: Planners are liable for the consequences they create.

Many of these characteristics arise since the problem is shared across multiple stakeholders with differing perspectives on the problem. Both of the EMBC programs share many of these characteristics which may have a great deal to do with the ambiguity of the goals for both programs.

Since the OR&A community stresses problem formulation in its Code of Best Practice, it is not surprising that a field within operational research has developed specifically to address problem formulation of wicked problems. This sub-field has been termed "soft" operations research (OR) to distinguish it from the "hard" OR that has primarily dealt with analyzing physical systems. Pioneers in the field of soft OR, Peter Checkland and Sue Holwell, explain the difference between hard and soft OR. Hard OR has an ontological perspective, takes the perceived world as a given and models it accordingly to identify solutions, while soft OR is epistemological, accepts that there are multiple, legitimate perspectives of the world and seeks to build common understanding and agreed action amongst stakeholders [10]. The general characteristics of soft OR are:

- Methodology: Based on rigorous epistemology (that is, a method understanding the difference perspectives for describing the world)
- Models: Represent varying concepts relevant to the real world
- Validity: Defensibly coherent, logically consistent, plausible
- Data: Based on judgement, opinion, some ambiguity, observer dependent
- Values and study outcomes: Agreement, shared perceptions, informing action and learning
- Purpose of the study: For the study – remains problematical; for the model – a means to learning.

A soft OR approach should elicit information from various stakeholders on their perceptions of the problem, organizes the information and then presents the information back to the stakeholders in a way that facilitates learning and the development of a shared perspective of the problem and ways in which they can agree on action to address the shared problem. Appling soft OR to a wicked problem will involve:

- Working across internal and external organizational boundaries;
- Engaging all stakeholders in policy development and implementation; and
- Facilitating the changing of the stakeholder group's behaviour.

The soft OR approach is a rigorous process for formulating problems that include multiple but legitimate stakeholder perspectives. The process is intended to produce shared perceptions of a problem or an understanding of the legitimate perspectives of other shareholders. It is a collective learning process which is iterative in application.

3 Risk Assessment

As per the NATO code, the first step in addressing the HRVA and CI programs is problem formulation. The same general approach was used for both programs. A preliminary literature review was conducted to identify tools/processes from other national approaches that may be of use in BC and to identify best practices, if they exist. Also conducted were stakeholder analyses, examination of the programs, and the elicitation of perspectives from stakeholders. This chapter presents supporting material. The subsequent chapter on CI has a similar structure.

3.1 Risk Management Literature Review

The goal of risk assessment is to "support risk management and policy decisions before the basic phenomena are fully understood, and in particular, to allow ranking risk reduction options on a cost-effectiveness basis" [11]. Risk assessment is intended as a tool to aid in decision-making, and has its foundations in probability theory. This literature review focuses on risk management/assessment standards and programs that have been developed including:

- The ISO 31000 International standard;
- National approaches to risk management, including those of the United States, the Netherlands, the United Kingdom, and Canada.

3.1.1 ISO 31000 International Standard for Risk Management

The ISO 31000 International Standard for Risk Management [12] was developed by a working group with representatives from 18 countries and is based on a widely-accepted and respected Australia/New Zealand risk management standard (AS/NZS 4360:2004). ISO 31000 was the primary reference document used for assessing requirements and gaps in EMBC's program. The document provides principles, a framework and a process for managing risk, as illustrated in the figure below. However, it does not provide details for a risk assessment.

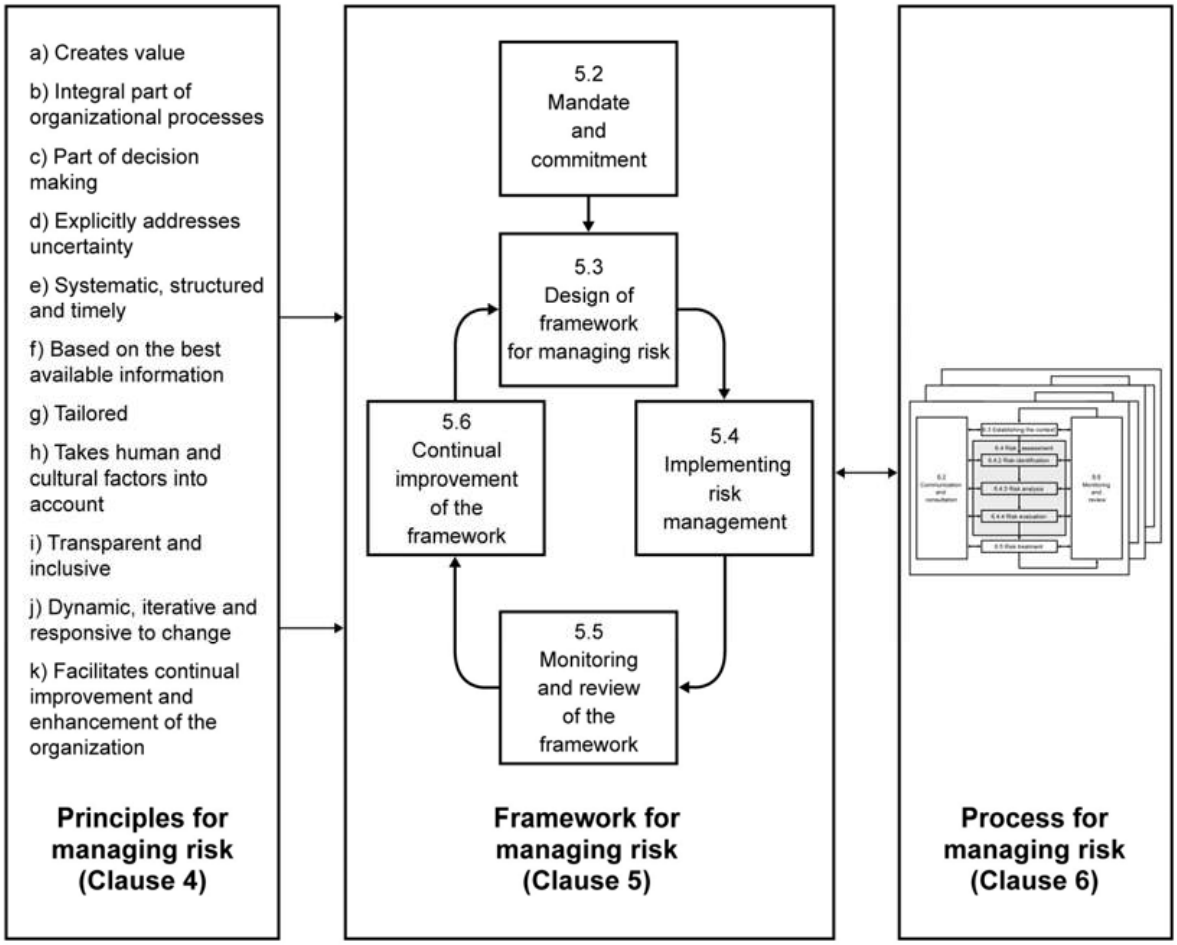

Figure 2. ISO Risk Principles, Framework, and Process for Managing Risk

The principles for managing risk are defined as follows (definitions are taken directly from the standard):

a) Creates and protects value: Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) Integral part of all organizational processes: Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

c) Part of decision making: Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) Explicitly addresses uncertainty: Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) Systematic, structured and timely: A systematic, timely and structured approach to risk management contributes to efficiency and consistent, comparable and reliable results.

f) Based on the best available information: The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) Tailored: Risk management is aligned with the organization's external and internal context and risk profile.

h) Takes human and cultural factors into account: The organization's risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

i) Transparent and inclusive: Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) Dynamic, iterative and responsive to change: Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) Facilitates continual improvement of the organization: Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

EMBC's program was compared against these principles to evaluate the status and assess gaps. The principles feed into a risk management framework, which includes a mandate and commitment, the design of the framework itself, the implementation of the risk management process, monitoring and review, and continual improvement.

The risk management process as defined in the standard is shown in the figure below.

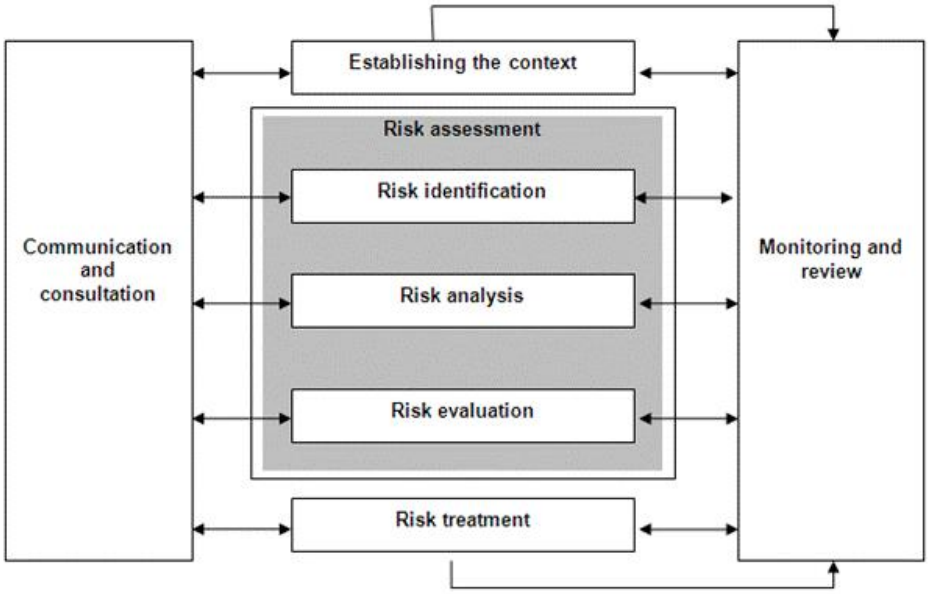

Figure 3. The ISO 31000 Risk Management Process

Risk assessment is defined as the overall process that includes:

- Risk identification - identifying hazards, events, situations, or circumstances that could cause risk;
- Risk analysis - developing an understanding of the risk, which involves an understanding of causes of risk along with the consequences and likelihood of events;
- Risk evaluation – involves prioritization of risks from the risk analysis (typically by comparing it with a risk criteria established as part of the context) in order to make decisions for risk treatment.

The risk assessment process is used to provide an improved understanding of risk and the effectiveness of controls in place. The outputs of the process are intended as inputs to an organization's decision-making processes. While EMBC's HRVA Tool Kit is titled as an analysis tool, in practice it is an assessment tool that encompasses identification and evaluation of risk.

3.1.2 A Review of the United States (US) Department of Homeland Security (DHS) Approach to Risk Analysis

The United States (US) Department of Homeland Security (DHS) was formed in response to the events of September 11, 2001 with a mission "to ensure a homeland that is safe, secure, and

resilient against terrorism and other hazards"[4]. DHS has a staff of more than 230,000 employees and a 2011 budget of almost $100 billion[5]. DHS responsibilities are to:

- Prevent terrorism and enhance security;
- Secure and manage borders;
- Enforce and administer immigration laws;
- Safeguard and secure cyberspace;
- Ensure resilience to disasters;
- Mature and strengthen DHS.

The US National Research Council was enlisted to review DHS' approach to risk analysis and published their findings in 2010 [13]. The committee reviewed six risk models and processes:

1. Risk analysis of natural hazards;
2. Risk analysis for critical infrastructure protection;
3. Risk analysis for allocation of homeland security grants;
4. Terrorism Risk Assessment and Management (TRAM) model;
5. Biological Threat Risk Assessment (BTRA) model; and
6. DHS's Integrated Risk Management Framework.

The review identified a number of significant deficiencies. The DHS conceptual risk framework itself, considering risk as function of threat, vulnerability and consequence, was concluded to be sound and appropriate for "decomposing risk and organizing information". Furthermore, the natural hazards risk analysis models, which focus on hurricanes, earthquakes, and floods, were concluded to be "near state-of-the-art"; that is, based on extensive data and validated empirically. However, the committee found the validity and reliability of models in the other areas to be untested and that the methods were not yet adequate to support DHS decision making. The primary report recommendation was that DHS strengthen its scientific practices, including documentation, validation, and peer review outside of DHS. The report also identified an urgent need to assess and communicate the uncertainty, assumptions, and variability within risk analyses. Furthermore, all-hazards risk assessment was concluded to be an impractical goal since the risk presented by terrorism and natural hazards cannot be combined into one meaningful risk metric. Therefore, the recommendation was that comparable risk analyses be performed rather than an integrated risk analysis that attempts to assess all risks against a common metric.

[4] http://www.dhs.gov/xabout/responsibilities.shtm
[5] http://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security

The US National Research Council is not alone with respect to concerns regarding risk analysis methodologies. Cox [14], for example, notes the lack of rigorous validation of the performance of risk matrices (that is, "tables mapping 'frequency' and 'severity' ratings to corresponding risk priority levels") in improving risk management decisions. He identifies the following limitations of risk matrices: (1) poor resolution; (2) errors; (3) suboptimal resource allocation; and (4) ambiguous inputs and outputs, and suggests that risk matrices be used with caution. Similarly, Hubbards and Evans [15] identify four problems with scoring methods and ordinal scales in risk assessment: (1) cognitive biases; (2) variability in verbal labels; (3) invalid inferences; and (4) invisible correlations. They propose that risk assessment methods should:

- Use explicit probabilities and quantitative magnitudes of losses instead of verbal or ordinal scales;
- Use Monte Carlo simulations to model systems components and correlations;
- Allow for corrective methods to be used for biases in human judgment.

3.1.3 The Dutch National Risk Assessment

The Dutch initiated a national risk assessment (NRA) process in 2004 for national safety and security to assist in planning for disasters. An NRA methodology team consisting of civil servants, scientists and consultants was established in 2007 [16]. The Dutch Ministry of the Interior and Kingdom Relations specified that the methodology was to be able to handle multiple criteria and be as transparent and methodologically consistent as possible.

Five "vital" interests to the state and society and their ten impact criteria were defined as follows [16, 17]:

- Territorial safety: infringement of: (1) the Dutch territorial integrity or (2) the integrity of the international position;
- Physical security: (3) number of fatalities, (4) number of injured and chronically ill, (5) physical suffering;
- Economic security: (6) financial costs;
- Ecological security: (7) long term damage to flora and fauna;
- Social and political stability: (8) disruption to everyday life, (9) violation of the democratic system, (10) social psychological impact.

The Dutch NRA process includes the use of three multi-criteria decision analysis (MCDA) methods in parallel and uncertainty, sensitivity and robustness analysis. In 2007, thirteen malicious and non-malicious scenarios were considered, from pandemic flu to Muslim extremism. The scenarios were each scored using the ten impact criteria and ordinal labels of 0 (not relevant) and A-E (limited to catastrophic impact). The team used three MCDA methods for ranking and classifying the scenarios because of the mix of qualitative and quantitative

evaluations: (1) the quantitative weighted sum method; (2) the ordinal Medal Methods; (3) and the ordinal variant of the Evamix method. Uncertainty, sensitivity, and robustness analyses were performed. In the end, "only the most important insights generated during the analysis" were communicated [16].

3.1.4 United Kingdom (UK) National Risk Assessment

The United Kingdom's National Risk Assessment is a classified risk assessment that has been carried out since 2005, and forms the basis of the public National Risk Register [18]. Historical and scientific data along with expert opinions are used to analyse risk to the UK. The analysis has three stages: risk identification, likelihood and consequence assessment, and a comparison of the risks.

The impact criteria are:

- The number of fatalities as a result of the emergency;
- Human illness or injury following the emergency;
- Social disruption, which includes ten types of disruption to daily life such as access to health care or the supply of essential services;
- Economic damage to the economy.

Psychological impacts are also estimated. Priority is given to high risks that are likely to occur and have significant impact. The figure below shows the risk diagram as presented in [18]. Human pandemic disease was considered to be the highest risk.

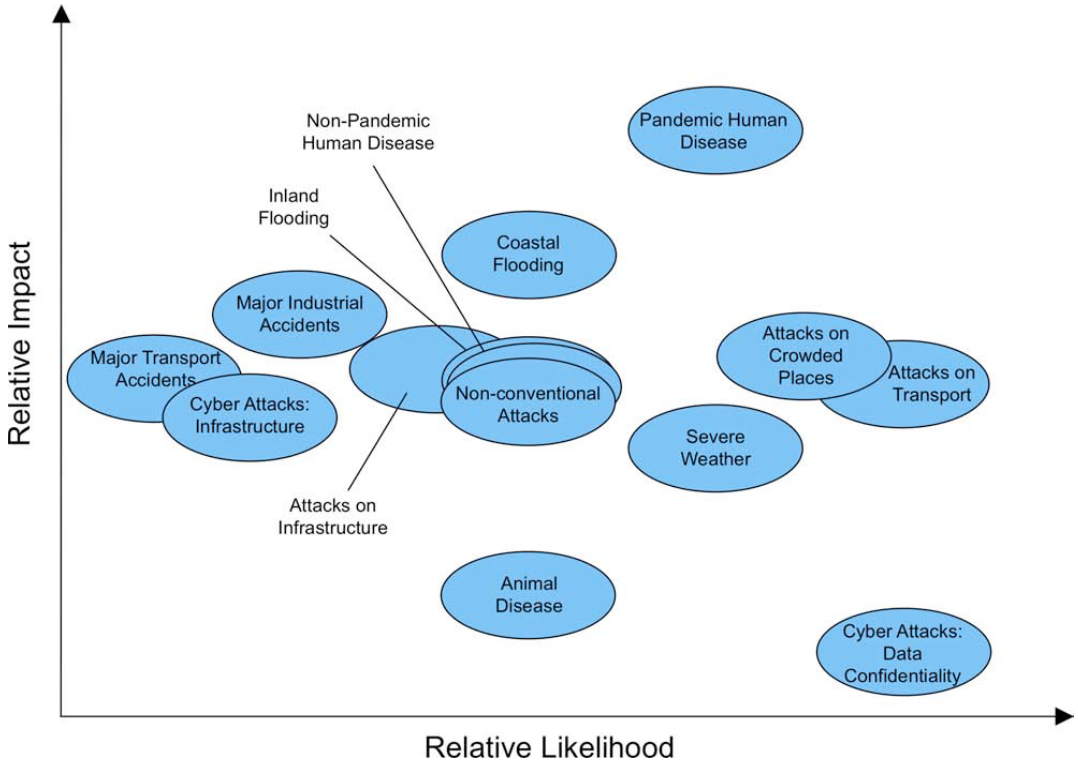

Figure 4. Risks Facing the United Kingdom

3.1.5 Risk Management in Canada

3.1.5.1 Treasury Board Secretariat (TBS) Guide to Integrated Risk Management

Treasury Board Secretariat (TBS) has developed a Guide to Integrated Risk Management [19] with a companion TBS Framework for the Management of Risk [20]. The guide is intended to assist federal departments with the design, implementation and improvement of integrated (organization-wide) risk management and references the ISO 31000 standard. A holistic approach is taken, covering:

- Risk management framework. The framework defines key concepts such as risk, risk management, integrated risk management, risk-informed approach, risk culture, and risk tolerance. Risk management principles are specified along with the roles and responsibilities of deputy heads and TBS;

- Plan and design of the approach and process. This includes understanding the organization and its context, establishing and articulating direction, accountability, resources, defining the risk management process - including risk identification, assessment, response, communication, monitoring - and communications and reporting mechanisms;

- Implementing integrated risk management. Implementation of the approach and process includes providing the environment and infrastructure and considerations such as culture, capacity, human resources, tools and techniques;

- Practicing integrated risk management and ensuring continuous learning;

- Improving integrated risk management, including monitoring and review.

3.1.5.2 Public Safety Canada (PSC) All Hazards Risk Assessment (AHRA)

In November 2009, the federal Assistant Deputy Minister (ADM) Emergency Management Committee (EMC) provided direction to Public Safety Canada (PSC) to develop the Federal All Hazards Risk Assessment (AHRA) by October 2011. The purpose of the AHRA is to support federal departments in meeting their legislative responsibility (under the Emergency Management Act) to identify risks within or related to their mandate and develop emergency management plans accordingly. In the spring of 2011, three pilot risk-scoring workshops were conducted on health hazards, natural hazards and national security threats. The intent is to complete a federal AHRA annually starting with the identification of threats and hazards each summer. Final results of the risk assessments will be maintained by PSC and disseminated to federal institutions involved in the AHRA.

The AHRA's objectives are to:

- "Enable federal government institutions to perform AHRA consistently and efficiently as part of their risk management responsibilities under the EMA and other relevant legislation and policies;

- Address the interconnected nature of Canada's risk environment and provide a means to produce a collective judgment of risk assessments currently being carried out by different federal government institutions into a whole-of-government picture to inform future actions and initiatives;

- Support the relative ordering of risk events based on their ratings at a federal level, while enhancing decision-making processes within the government of Canada;

- Capture risks that are significant and are of federal interest;

- Raise awareness of risks that may not be of federal concern at this time, but are likely to be elevated in the future;

- Raise awareness of risks that are not of federal concern, but ensure that these risks are monitored;

- Capture changes in risks over time;

- Help to foster an AHRA community of practice for the federal community." [21]

The AHRA consists of a five step process of: (1) setting the context, (2) risk identification, (3) risk analysis, (4) risk evaluation, and (5) risk treatment.

The main objective for setting the context is to "develop a comprehensive understanding of the strategic and operating context of an organization" [21]. Sources of information are cited as departmental planning and reporting documentation, environmental scans, historical records, and intelligence reports. The outputs of this step include an analysis of short-term (within five years), emerging and future (five to 25 years) threats and hazards. Following setting the context, the risk identification step identifies high priority threats and hazards (or risks) for each federal government department and associated scenarios to be used in risk analysis.

For the risk analysis, the likelihood and impact of malicious and non-malicious threats and hazards are considered. Six impact categories are defined:

- People – fatalities and "fatality-equivalents" following a risk event;
- Economy – direct and indirect economic loss in dollars;
- Environment – considers the magnitude of a response required to deal with a situation, the geographical extent of the damage, the magnitude of damage based on adverse effects to different components of the environment, and the duration of the damage including the level of recovery efforts.
- Territorial security – loss of the ability to control Canadian territory;
- Canada's reputation and influence – reflects potential international reaction;
- Society and psycho-social – considers evidence of social actions and public mood.

Impact categories are evaluated either in terms of quantitative (for example, lives and dollars) or qualitative scales. Likelihood assessments are made based on historical data, predictive models, or expert judgment for non-malicious threats, and assessments of technical feasibility, capability, and intent for malicious threats.

The risk evaluation is a comparison of individual likelihood and impact assessments in risk diagrams or risk rating matrices. A sample risk event rating scatter plot is shown in the figure below, where each dot represents the results for a scenario considered and the bars the corresponding uncertainty of the results.

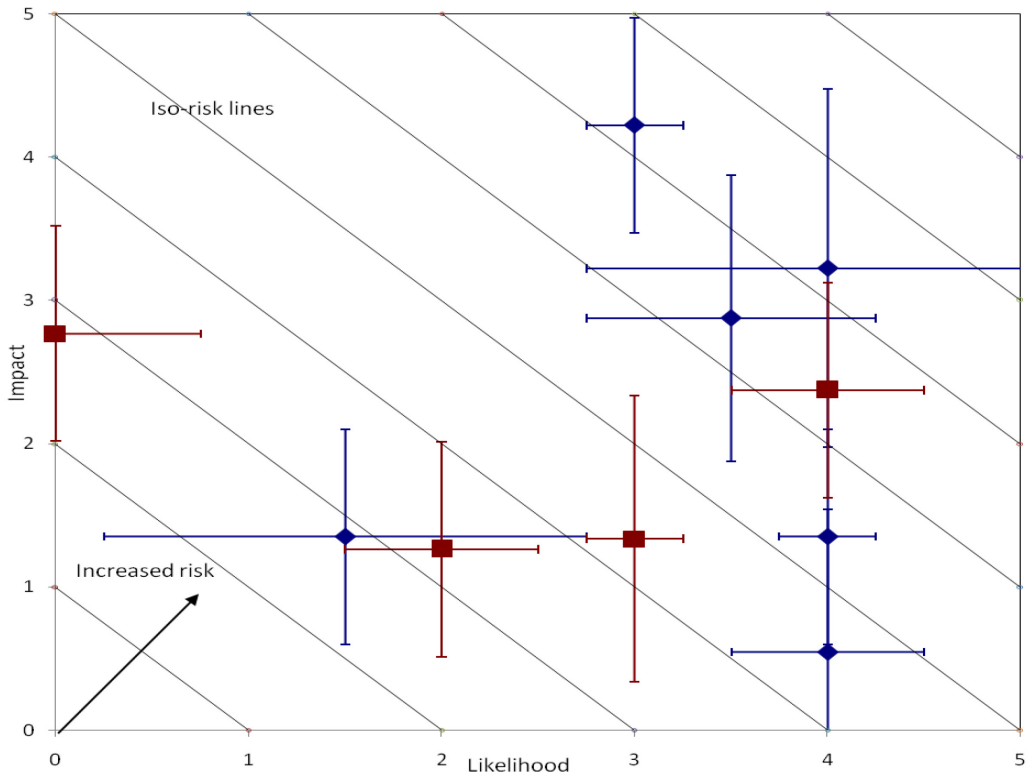

Figure 5. Risk Event Rating Scatter Plot

3.2 EMBC Hazard Risk Vulnerability Analysis (HRVA) Program

According to the NATO Code of Best Practice for C2 Assessment, problem formulation involves interactions with the stakeholders to characterize the context, identify key and "real" issues, and characterize key elements [4].

3.2.1 Stakeholder Analysis

3.2.1.1 Community Stakeholders

The primary responsibility for risk assessments lies with local authorities. The BC Emergency Program Act (EPA) [22] mandates the use of risk assessments for local authorities (communities) in order to develop emergency plans. However, these community risk assessments should involve multiple groups, such as local government representatives (emergency coordinators, council members, planning, engineering departments), emergency professionals (police, fire, ambulance, etc.), critical infrastructure owners, various subject matter experts (for example, on hazards and threats), and other members of the community (for example, from volunteer groups). The degree

of engagement of all these groups in community risk assessments is likely dependent on the community, the resources for completing risk assessments, a willingness to work together, etc.

In some communities the emergency program coordinator may be a dedicated, full-time position with additional staff resources, while in others the responsibility may be one of many under another position - sometimes even a volunteer position, such as the volunteer fire chief. Therefore, the amount of time and resources available to dedicate to activities such as risk assessment can vary widely.

Within municipalities and regions, there are various departments that have roles related to risk assessment and emergency management, such as land use planning, engineering departments, emergency programs, etc. However, these functions are often not integrated and these groups do not necessarily communicate regularly or coordinate with one another.

3.2.1.2 EMBC

EMBC provides training and support to local governments for emergency management. EMBC is comprised of five strategic business units: (1) Strategic Planning, Policy, and Legislation; (2) Mitigation; (3) Emergency Coordination; (4) Corporate Services; and (5) BC Coroners Service[6]. The province is divided into six regions: (1) Vancouver Island, (2) Southwest, (3) Southeast, (4) Central, (5) Northeast, and (6) Northwest. Regional managers (RMs), part of the Emergency Coordination business unit, are responsible for those communities within their region and maintain profiles for each community. They generally have copies of community emergency plans and contact local authorities annually (at a minimum) for updates to emergency plans. The RMs may or may not have copies of risk assessments (RAs) since it is at the discretion of the community to share RAs. These same regional managers staff key positions (such as director) in Provincial Regional Emergency Operations Centres (PREOCs) and the Provincial Emergency Coordination Centre (PECC) in Victoria during emergency response when PREOCs are activated in support of local authorities.

EMBC is responsible for the emergency management cycle of mitigation and prevention, preparedness, response and recovery. However, given limited resources and budgets, the focus is often heavily on response; in fact, other duties and projects get put on hold in times of emergency response for EMBC employees who man operations centres. During emergency events such as annual flooding and wildfires, all RMs may be required to staff PREOCs and the PECC, working long hours. During large activations, EMBC may struggle to fully staff these operations centres over extended periods.

EMBC's Strategic Planning, Policy and Legislation business unit is comprised of four teams: (1) Integrated Planning; (2) Catastrophic and Recovery Planning; (3) Business Continuity Planning; and (4) Integrated Public Safety (IPS) [25]. These teams are small in size, generally ranging from two to five EMBC employees. IPS was created for V2010 with the majority of its personnel seconded from other departments and agencies. At the end of the games most seconded personnel (such as the first author) returned to their home organizations. A case was made within EMBC for the continued existence of IPS and two full-time positions were kept. In addition, IPS has been building a team of (mostly part-time) subject matter experts (SMEs) (from, for example, BC

[6] http://www.bcaem.ca/en/BCAEM_News_28/items/13.html

Coroner's Service, BC Ministry of Health, RCMP), with a similar secondment model as was used for V2010. Despite the fact that all hazards planning and HRVA fall under the Integrated Planning team according to EMBC documentation [25], this project was undertaken with IPS with the blessing of the executive director of the unit.

3.2.2 EMBC HRVA Tool Kit and Other Risk Assessment Work

EMBC developed the HRVA Tool Kit in 2004 to "help a community make risk-based choices to address vulnerabilities, mitigate hazards and prepare for response to and recovery from hazard events" [23]. The tool kit guides users through a risk assessment process, from hazard and vulnerability identification to risk analysis to action plans, and has been used by many communities to develop risk assessments. There is an online version as well as a downloadable paper version.

At the request of the Executive Director of EMBC's Strategic Planning, Policy and Legislation business unit, DRDC provided "quick look" feedback on the HRVA Tool Kit in early 2011 [24]. It was intended that a more detailed assessment would be provided as a component of the subsequent HRVA assessment. However, the initial response was considered to be sufficient by EMBC and, therefore, the assessment focused at the program level.

Other risk assessment work in BC includes:

- Risk assessments completed by contractors or local authorities (LAs) using a methodology other than the HRVA Tool Kit;
- A 1997 Provincial HRVA completed by Laurie Pearce;
- "Introduction to Hazard and Risk Management" course provided by the Justice Institute of British Columbia (JIBC) ;
- Components of a current CRTI project "Building Resilience and Rural Health System Capability for Pre-Disaster Planning and Preparedness" led by the Justice Institute of BC in partnership with the Public Health Agency of Canada, with contributions by Laurie Pearce and Robin Cox;
- Natural Resources Canada's development of a framework for integrated assessment and risk-based planning associated with natural hazards, including the Canadian application of the US Federal Emergency Management Agency (FEMA) HAZUS methodology, with a case study in Squamish, BC [56];
- The DRDC CSS-led Consolidated Risk Assessment workshop. The Capital Regional District (Victoria) held a workshop in February 2011 and the Integrated Partnership for Regional Emergency Management (IPREM) hosted workshops for Metro Vancouver in November 2011 and February/March 2012;
- This collaborative project between EMBC and DRDC.

3.2.3 Elicitation of Perspectives

EMBC and DRDC conducted three teleconference sessions to interview regional staff from the six regions of EMBC:

- Session 1: Vancouver Island and Southwest;
- Session 2: Southeast and Central;
- Session 3: Northeast and Northwest.

The purpose of the interviews was to understand how the EMBC HRVA Tool Kit was being used across the province, how HRVA processes were being applied to planning and what regional staff would like to see going forward.

The following questions were prepared by EMBC and DRDC for discussion and distributed in advance to the regional offices:

- What are the current emergency management priorities for your region and how has the HRVA process been incorporated into these priorities?
- What risk assessments have been done in your region, by local authorities and/or other key stakeholders?
    - How familiar are you with the HRVA Tool Kit?
    - Are local authorities and stakeholders using the HRVA Tool Kit? Have you recommended it to local authorities?
    - Have you received any results that have come from this tool?
    - What were the results of the risk assessments? Or, what would you expect them to be?
    - How have the results of the risk assessments been used? Or, how would you expect them to be used?
    - What resources (information, tools, personnel, etc.) were used?
- What has gone well with the risk assessments that have been done?
    - What do users like about the process? What are the positive aspects of the HRVA Tool Kit?
- What would you like improved?
    - What improvements to the HRVA Tool Kit have the users suggested?
    - What additional resources would you like to have access to in order to support HRVA in your region (information, qualified/knowledgeable personnel, tools, etc.)?
    - What improvements could be made in how the results of local risk assessments could be used to improve emergency management in your region?

- Additional Comments

Questions were also provided for RMs to provide to local authorities if they chose to do so:

- What are the current emergency management priorities for your region and how has an HRVA process been incorporated into these priorities?
- Have you done a risk assessment?
    - Have you used or are you familiar with the HRVA Tool Kit on the PEP website?
    - What other processes for conducting HRVA's have you used?
- List the things that you liked or would have liked improved with the HRVA methodology(s) you have used.
- What improvements could be made in how the results of risk assessments could be used to improve emergency management in your region?
- Additional Comments

A few RMs sent these questions to local authorities within their region and provided feedback on them during the interview. Responses to the questions were one of the primary sources of data for the evaluation of gaps in the EMBC program. RMs reported that there was a move towards regional planning but that existing tools did not support regional risk assessments. Furthermore, a "one size fits all" approach was clearly not sufficient to meet the needs of the various communities and regions.

3.2.4 Status of the EMBC HRVA Program

The EMBC HRVA program was assessed by the authors for requirements and gaps. The ISO 31000 [12] standard on risk management was used as a baseline for assessing the HRVA program. The standard is intended for stakeholders who:

- Are responsible for developing risk management policy in their organization;
- Are accountable for ensuring that risk is effectively managed within their organization, area, or project;
- Need to evaluate effectiveness in managing risk for an organization;
- Develop standards, guides, procedures, etc. related to managing risk.

While the standard is intended primarily for single-entity organizations and community risk assessments include a wide range of stakeholders, the principles were deemed to be applicable for risk management in general. As outlined in the HRVA literature review section, ISO 31000 outlines a framework, principles and a process for risk management. In using the ISO standard as a baseline, a number of gaps were identified in the HRVA program. These gaps were grouped into five categories of:

1. Risk management framework;

2. Regional HRVA;

3. Measurement and validation;

4. Partnerships; and

5. Training.

The specific gaps are not included in this report due to the sensitive nature of the information. Further detail on the analysis and results is contained in the EMBC client letter report [26].

4 Critical Infrastructure (CI)

This chapter is organized in the same way as the previous chapters, starting with a literature review and followed by stakeholder analysis and EMBC program review.

4.1 CI Literature Review

The literature search to date has covered:

- National strategies of Canada and other nations, such the United States (US), the United Kingdom (UK), and Germany;
- The US National Incident Management System (NIMS) including the Target Capability List;
- Academic research on CI interdependencies;
- Risk Management Standards (ISO 31000);
- Practitioner recommendations for public-private partnerships.

These documents provide a substantial body of both theoretical and practical experience on best practice.

4.1.1 United States' Approach to CI

The United States has eighteen critical infrastructure and key resource sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defence industrial base; emergency services; energy; government facilities; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water. The US has a lot of resources and money dedicated to CI protection and therefore a number of standards, guidelines, plans, and programs. This section outlines several of them at a high level.

The US published a National Strategy for the Physical Protection of Critical Infrastructure and Key Assets in early 2003 in response to 9/11 when the protection of key assets from terrorist attacks became a priority [27]. The strategy established "a foundation for building and fostering a cooperative environment in which government, industry, and private citizens can work together to protect our critical infrastructures and key assets", outlining goals objectives, and guiding principles, defines roles and responsibilities, and identifying major initiatives for CIP. DHS houses the Office of Infrastructure Protection[7], whose mission is to protect the nation's infrastructure. They are the sector-specific agency (SSA) for six of the eighteen CI sectors, including chemical; commercial facilities; critical manufacturing; dams; emergency services; and

[7] http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm

nuclear reactors, materials, and waste. DHS has a host of infrastructure protection programs[8], such as:

- Automated Critical Asset Management System (ACAMS);
- Borders & Maritime Security Projects;
- Chemical Security;
- Cyber security;
- Federal Building Security;
- Homeland Security Information Network;
- Information Sharing;
- National Infrastructure Coordinating Center;
- TRIPWire (Bombing Prevention and Awareness);
- Bomb-Making Materials Awareness Program (BMAP);
- Partnerships & Councils;
- Protected Critical Infrastructure Information (PCII) Program;
- Protective Security Advisors;
- Secure Freight Initiative.

In a 2009 CI resilience report [29], the National Infrastructure Advisory Council found that some CI may be better served by adopting a resilience approach that focuses on the restoration of services in the event of a disruption, rather than on simply protection-based strategies. To this end, a number of recommendations were made in the report, including items such as defining a common definition with a strategy for funding and developing resilience, creating market incentives for encouraging resilience, improving coordination and clarifying roles and responsibilities of CI partners, strengthening and leveraging private-public relationships, and exercising across all partners.

4.1.1.1 National Infrastructure Protection Plan (NIPP)

The 2009 National Infrastructure Protection Plan (NIPP): Partnering to Enhance Protection and Resiliency "provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels,

[8] http://www.dhs.gov/files/programs/critical.shtm

the private sector, nongovernmental organizations, and international partners" [28]. The NIPP includes:

1. A delineation of the roles and responsibilities for CI partners and a description of the key tasks that should be performed by each partner;

2. A risk analysis and management framework that establishes the required processes. The framework is intended to focus "activities on efforts to set goals and objectives; identify assets, systems and networks at risk based on consequences, vulnerabilities and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness."

3. The definition of organizational structures to provide a framework for coordination;

4. Recognition that CI protection is an integral component of the homeland security mission. The plan, therefore, includes guidance on plan structure and content with the intention that this will "provide a baseline framework that informs the flexible and tailored development, implementation, and updating of" plans and strategies;

5. Provisions to ensure an effective, efficient program over the long term; and

6. Resources to aid the implementation of the plan.

SSAs, the federal agencies that lead CI collaboration within a sector, have developed sector-specific plans[9] in accordance with the NIPP.

4.1.1.2 National Incident Management Standard (NIMS)

The 2004 National Incident Management Standard is a unified national approach for incident management, created to provide compatibility and interoperability between federal, state, and local governments [30]. The NIMS components are:

- Command management, including the incident command system (ICS), multiagency coordination systems, and public information systems;

- Preparedness, including planning, training, exercises, personnel, equipment, mutual aid, and publications management;

- Resource management;

- Communications and information management;

- Supporting technologies; and

- Ongoing management and maintenance.

[9] Available from http://www.dhs.gov/files/programs/gc_1179866197607.shtm

NIMS adopts best practices for a consistent approach to all hazards incidents across jurisdictional levels. Part of the NIMS approach includes the creation of a "capability" taxonomy, which is termed the Target Capability List (TCL). Further information can be found below in the section describing the TCL.

4.1.1.3 National Preparedness Guidelines

The 2007 National Preparedness Guidelines vision is, "A nation prepared with coordinated capabilities to prevent, protect against, respond to, and recover from all hazards in a way that balances risk with resources and need" [31]. The purpose of the guidelines is to strengthen preparedness by organizing and synchronizing national efforts, guide national preparedness investments, facilitate a risk and capability-based investment planning process, incorporate lessons learned from past events, and establish metrics and a system for assessing preparedness to respond to major events. The priorities defined by the guidelines are:

- Expanding regional collaboration;
- Implementing the National Incident Management System and National Response Plan;
- Implementing the National Infrastructure Protection Plan;
- Strengthening information sharing and collaboration capabilities;
- Strengthening interoperable and operable communications capabilities;
- Strengthening CBRNE Detection, Response, and Decontamination Capabilities;
- Strengthening medical surge and mass prophylaxis capabilities;
- Strengthening Planning and Citizen Capabilities.

The NPG provides an example of overarching guidelines and priorities that are needed to facilitate collaboration and coordinate more detailed planning amongst the stakeholder community.

4.1.1.4 Target Capabilities List (TCL)

The Target Capabilities List (TCL) [32] is a guide for achieving the priorities of the National Preparedness Guidelines. The TCL defines a number of common capabilities, "prevent" mission capabilities, "protect" mission capabilities, and "respond" mission capabilities. CI is considered as one of its "protect" mission capabilities.

The capability definition for critical infrastructure protection is defined as follows:

- "The Critical Infrastructure Protection (CIP) capability enables public and private entities to identify, assess, prioritize, and protect critical infrastructure and key resources so they

can detect, prevent, deter, devalue, and mitigate deliberate efforts to destroy, incapacitate, or exploit the Nation's critical infrastructure and key resources."

With the outcome:

- "The risk to, vulnerability of, and consequence of an attack on critical infrastructure are reduced through the identification of critical infrastructure; conduct, documentation, and standardization of risk assessments; prioritization of assets; decisions regarding protective and preventative programs; and implementation of protective and preventative plans." [32]

Preparedness and performance tasks, measures, and metrics are outlined for CIP. Preparedness measures include the development and maintenance of plans, procedures, programs, systems, training and exercise programs. Performance measures include coordinating and managing CIP; identifying critical infrastructure/key resources (CI/KR); assessing risks; prioritizing high-risk CI/KR; protection of CI/KR; and measures of effectiveness.

4.1.1.5 CARVER

The CARVER matrix[10] was developed by the US military during the Vietnam War to aid in identifying the attractiveness of targets that are vulnerable to attack. CARVER is an acronym for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognisability. Assets are typically scored on a scale of one to ten (one being low attractiveness or vulnerability and 10 being high) across these categories and total scores compared between assets.

The US Food and Drug Administration has developed a free Vulnerability Assessment Tool[11] for the food sector using the CARVER attributes defined above plus the a seventh "Shock" attribute that considers health, economic and psychological impacts. The tool is intended for use by state and local food security agencies, industrial providers, and food processors.

The US National Infrastructure Institute has developed the "CARVER2" infrastructure analysis system[12] with a free web tool based on the CARVER matrix to help with the prioritization of CI assets and resources. The analysis categories used are: Criticality, Accessibility, Recoverability, Vulnerability, Espyability[13], and Redundancy.

4.1.2 United Kingdom's Approach to CI

The United Kingdom (UK) has nine CI sectors: communications; emergency services; energy; finance; food; government; health; transport; and water. The UK distinguishes between critical infrastructure (CI) and critical national infrastructure (CNI), the difference being that CNI has been identified as being critical on a national scale.

[10] http://en.wikipedia.org/wiki/CARVER_matrix
[11] http://www.fda.gov/Food/FoodDefense/CARVER/default.htm
[12] http://www.ni2cie.org/CARVER2.asp
[13] This is defined as "notoriety"; that is, is the infrastructure is an icon representing more than a physical structure (such as a national monument)?

The UK addresses security threats and natural hazards separately:

- The Centre for the Protection of National Infrastructure (CPNI)[14] provides security advice for reducing the vulnerabilities of critical national infrastructure with a focus on terrorism and other threats to national security [34].

- The Civil Contingencies Secretariat addresses the resilience of CI with respect to natural hazards. The Critical Infrastructure Resilience Programme aims to reduce risk to CI from disruption caused by natural hazards; provide a shared framework for cross-sector activity related to natural hazards; enhance collective capacity to absorb and respond to unexpected events; ensure effective emergency response at the local level.

Sir Michael Pitt's report on the 2007 summer floods identified a gap in the government's program to address CI disruption from natural hazards. Subsequently, a 2010 statement [33] from the Cabinet Office outlined a strategic policy and framework to improve the resilience of CI from natural hazards.

A framework and guidance for protecting infrastructure has been developed [34]. The framework includes a criticality scale that defines six categories of disruption or failure for essential services, as shown in the table below, from minor to catastrophic.

Criticality Scale	Description
Category 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria.
Category 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens.
Category 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people.
Category 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents.
Category 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens.
Category 0	Infrastructure the impact of the loss of which would be minor (on national scale).

Table 1. Criticality Scale Description [33

The criticality scale is further defined across three "impact dimensions": (1) impact on life in terms of casualties and fatalities; (2) economic impact in pounds; and (3) impact on delivery of essential services. The essential services are broken down yet even further, defining what constitutes each category of failure for each of the nine CI sectors (for example, what constitutes a Category 0, 1, 2, 3, 4, and 5 failure in the energy sector is specifically defined) [35]. The highest degree of criticality determines the overall criticality impact for the CI. The criticality scale is

[14] http://www.cpni.gov.uk/

then used to define critical "national" infrastructure (CNI) by setting a threshold – if the impact of loss of infrastructure falls above the threshold then that infrastructure is considered to be CNI. The threshold is currently set at Category 3, that is, CI in Categories 3-5 is CNI [33]. Sector sponsor departments have the lead on identifying what may be critical within their sector.

The Civil Contingencies Act 2004 designates many of the owners of CI and providers of essential services as either Category 1 (for example, emergency services and local authorities) or Category 2 responders (for example, utilities with the exception of electricity generators). Under the act cooperation and information sharing responsibilities are defined at a high level.

4.1.3 Germany's Approach to CI

Germany has nine CI sectors: energy; finance; food; government; health and insurance industry; information technology and telecommunications; media and culture; public administration; transport and traffic; and water[15]. Germany's guiding principles for critical infrastructure protection (CIP) are: (1) trust and cooperation between government, business, and industry at all levels and (2) the requirement and suitability of measures for increasing CIP [36]. An implementation procedure has been defined, which includes threat and vulnerability analysis, identification of targets for protection, the implementation of measures for goal attainment, and a continuous risk management process.

4.1.4 Canada's Approach to CI

Public Safety Canada (PSC) has defined ten CI sectors: energy and utilities, food, finance, government, health, information and communications technology, manufacturing, safety, transportation, and water [37]. The National Strategy [37] and Action Plan for CI [38] identify three strategic objectives of:

1. Building partnerships;
2. Improving information sharing and protection;
3. Implementing all hazards risk management.

A three year plan was developed that relies on work being done within sector networks, and defines a federal lead for each sector. In addition, a 2010 Canada-United States Action Plan for Critical Infrastructure [39] focuses on the above objectives.

4.1.5 Academic Research on CI Interdependencies

In Canada, there are two main groups modelling CI interdependencies, one at the University of British Columbia and the other at École Polytechnique de Montréal.

15 https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/Introductionandoverview/Criticalinfrastructuressectors/criticalinfrastructuresectors_node.html

4.1.5.1 Infrastructure Interdependencies Simulation (i2Sim)

Researchers at the University of British Columbia, led by Jose Marti, have used a systems engineering approach to simulate critical infrastructure interdependencies using the Infrastructure Interdependencies Simulation (i2Sim) [40], a toolbox built on Matlab. The underlying model uses cells (production units), channels (transportation units), tokens (exchange units), and controls (distributor and aggregator units) to create an input/output model representing and simulating different types of infrastructure. The i2Sim model considers various modes of operability of infrastructure as a result of damage, ranging from 0-100% operability, and simulates the effects of reduced operability over time. This allows for the identification of, for example, interdependencies and cascading effects, and multiple simulations can be run examining the effects of varying impacts on operability over time.

4.1.5.2 École Polytechnique de Montréal

Benoit Robert's team at the École Polytechnique de Montréal Centre risque & performance developed an approach to risk management for infrastructure interdependencies [41]. The approach has been developed in collaboration with public and private sector partners in the City of Montreal such as Bell Canada, GazMetro, Hydro Quebec, Minstere de la Security publique du Quebec, Ministere des Transport du Quebec, Public Safety Canada, Tecsult, and the City of Montreal. The premise is that information is exchanged between organizations in a "cooperative space" that allows each organization to develop an increased understanding of their dependencies and others' dependencies on them. Organizations must identify their degrees of infrastructure and resource essentiality, period of need, storage and alternative resources, and autonomy. The correlation of information allows for the exposure of cascading effects over time.

4.1.6 Risk Management and Private-Public Partnerships

Enhancing CI resilience is a form of risk management in that, according to ISO 31000 [12], it requires a process for "identifying, analyzing, evaluating and treating risk" faced by an organization in the achievement of its objectives. As described above ISO 31000 provides recommendations for best practice that include principles of an effective risk management process.

The ISO 31000 recommendations are primarily intended for implementation by an organization or a well-defined association of organizations. This was recognized by the US National Infrastructure Advisory Council in its report, *Critical Infrastructure Resilience: Final Report and Recommendations* [29], since the majority of their recommendations are directed at the management of risk management amongst government and CI owners and operators. The six key recommendations of the report were:

1. Fortify government policy framework to strengthen CI resilience;
2. Improve government coordination to enhance CI resilience;
3. Clarify roles and responsibilities of CI partners;

4. Strengthen and leverage public-private partnership;

5. Encourage resilience using appropriate market incentives; and

6. Implement government enabling activities and programs in concert with CI owners and operators.

Partnerships are emphasized in the US *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resilience* [28]. Effective public-private partnerships are essential for enhancing CI resilience. Private-public partnerships are not new as these have been implemented by governments at all levels as an alternative means of delivering services to the public. Goldsmith and Eggers set out recommendations for effective and efficient management public-private partnerships in *Governing by Network: The New Shape of the Public Sector* [42]. They make the point that:

> "The era of hierarchical government bureaucracy is coming to an end. Emerging in its place is a fundamentally different model – governing by network – in which government executives redefine their core responsibilities from managing people and programs to coordinating resources for producing public value."

Goldsmith and Eggers identify the advantages of public-private partnerships (that is, governing by network) as encouraging innovation, allowing government to concentrate on leveraging "best of breed" providers, enhancing flexibility and allowing for decentralized decision-making to the most appropriate level. However, there are challenges to effectively managing public-private partnerships that include the fact that poor performance by any one organization could imperil the performance of the whole and that:

> "Successful network management requires grappling with skill-set, technology, information asymmetry, cultural issues. The network manager must master the challenges of governing by network: aligning goals, providing oversight, averting communication meltdown, coordinating multiple partners, managing the tension between competition and collaboration, and overcoming data deficits and capacity shortages."

Lessons learned from experience show that the success or failure of a public-private partnership is often due to its original design. Goldsmith and Eggers identify a strong network integrator as a critical component of a successful partnership. However, even successful partnerships must deal with the most difficult challenge of accountability when authority and responsibility are distributed across the partnership. The design must clearly define the public good that is to be produced by the partnership and who is to be held accountable for what and by whom. "Government expectations must be specific enough to enable the network [that is the public-private partnership] to deliver services [that is, in this case enhanced CI resilience] effectively, but without saddling participants with counterproductive and unnecessarily detailed procedures." Goldsmith and Eggers put an emphasis on agreed important values and clarity of outcomes coupled with flexible processes.

4.2 EMBC Critical Infrastructure Assurance Program (CIAP)

As with the HRVA program, the problem formulation regarding EMBC's CIAP involved stakeholder analysis, an examination of the program itself, and an elicitation of perspectives from stakeholders.

4.2.1 Stakeholder Analysis

The CI stakeholder community can be represented by Canada's ten CI sectors: energy and utilities, food, finance, government, health, information and communications technology manufacturing, safety, transportation, and water. CI assets are often owned and operated by private sector companies, who are concerned about proprietary information and do not have a legal obligation to share information. Public Safety Canada has introduced regulations to protect CI asset owner information under the federal Emergency Management Act but this is applicable only to the sharing of information with *federal* organizations for specific purposes (for example, for the preparation, maintenance, testing or implementation of emergency management plans[16]). EMBC does not have similar regulatory protection. Therefore, in BC, "sensitive" information is typically only shared during the response phase of emergency events at the discretion of asset owners. However, during Vancouver 2010, a non-disclosure agreement (NDA) was put in place with the ISU in order for CI asset owners to share information for planning purposes. The type and quantity of data that was shared was voluntary and the data was destroyed post-Games under the agreement. In addition, information amalgamated for the analysis was designated as Secret by a blanket statement in the NDA, which resulted in the data and analysis generally not being sharable beyond the ISU.

EMBC chairs the BC CI Steering Committee, which brings together representatives from government/agencies at the local, regional, provincial and federal levels as well as private sector stakeholders. The Steering Committee is currently defining its terms of reference and working on establishing leads for provincial sector working groups. The Integrated Partnership for Regional Emergency Management (IPREM) is a partnership between the province and the 23 local authorities that comprise the Metro Vancouver region, with a mission to "develop and deliver a coordinated seamless regional emergency management strategy supported by an integrated concept of emergency operations, strategic priorities and supporting plans" [45]. IPREM was moved under IPS in 2011 to create more synergy between the work of IPREM and EMBC. One of IPREM's priority initiatives for 2011-2012 is to enhance CI assurance. While no private organizations can be members of the IPREM Steering Committee, private agency participation is invited and encouraged on many of the IPREM project working groups, such as the CI Assurance Working Group (WG). The IPREM CI Assurance WG utilizes the provincial CI assessment methodology and helps to promote and coordinate CI awareness with stakeholders in the region. IPREM was heavily involved with the development of the EMBC CI rating workbook including the consequence of loss tool. A number of the IPREM CI WG members are also on the provincial CI steering committee. Many organizational representatives face the challenge of being their organization's sole CI representative (or one of only a few) on multiple bodies with overlapping responsibilities.

[16] http://www.publicsafety.gc.ca/prg/ns/ci/_fl/information-sharing-and-protection-under-the-ema-eng.pdf

First responders and emergency management organizations are responsible for public safety and security while other stakeholders generally provide goods and services and are recipients of safety and security services. Interestingly, in an analysis of the CI data provided by approximately 125 asset owners on 5000 assets for V2010, overall only a very small number (roughly 1%) of owners identified dependencies on the safety sector.

4.2.2 CIAP

EMBC has proposed a Critical Infrastructure Assurance Program (CIAP) "to provide a framework for enhancing the resiliency of critical infrastructure in BC by promoting partnerships, information sharing, sound risk management and business continuity planning among CI stakeholders" [43]. EMBC does not have an employee dedicated full time to the CI program, rather it is the responsibility of the Director of IPS along with the IPS Emergency Management Planning Coordinator.

The objectives of the program are to:

- Enhance public safety;
- Promote inter-agency information sharing;
- Develop sustainable partnerships with key stakeholders;
- Produce and utilize point of contact list to track and map contact information and provide threat/hazard notification to stakeholders;
- Promote all hazard risk management; and
- Provide a common province-wide methodology for identifying and analyzing CI.

In addition to the above, the proposed CIAP concept emphasizes the need for a strong educational component and proposes building upon initiatives started during the planning and preparations for the Vancouver 2010 Olympic and Paralympic Games. These initiatives included building strong relationships with CI stakeholders and the development of tools such as:

- Mapping tools used in the Provincial Emergency Coordination Centre (PECC) and Provincial Regional Emergency Operations Centres (PREOC) for centralized CI advanced planning;
- A CI Spatial Query (CISQ) tool for notifying CI asset owners and operators of events in areas of interest to them; and
- A Critical Infrastructure Identification and Rating Workbook [44], including a Consequence of Loss (CoL) tool, for use by CI asset owners and operators to identify their most important assets, the loss of which would seriously affect their own operations, other CI asset owners and operators and society in general.

4.2.2.1 EMBC CI Rating Workbook and Consequence of Loss Tool

EMBC developed a Critical Infrastructure Rating Workbook [46] for freshet flooding in 2007. In the spring of 2008, a modified version was published for use for V2010 [44] and CI owners were engaged to identify and rate CI assets supporting both the region and the operation of the Games. Additionally, the output from this initiative was intended to assist CI asset owners/operators in the development of hazard risk vulnerability assessments, business continuity planning, risk mitigation and management, physical and information security, and information assurance.

The rating systems relies on the assessment of assets, using the following table to assign impacts across various factors and summing the impact score for a final asset rating (considering all hazards and maximum credible damage to an asset):

Impact Factor	Severe	Very High	High	Medium	Low	Very Low
Score	**15**	**5**	**3**	**1**	**0.5**	**0.1**
Population Impact • Estimate number of possible fatalities, serious injuries or people evacuated due to loss of asset being ranked. • Do not include people inconvenienced. • Consider maximum credible damage only.	Greater than 10,000 people	Between 1,000 and 10,000 people	Between 100 and 1000 people	Between 50 and 100 people	Between 4 and 50 people	Less than 4 people
Recovery Cost Impact • Estimate cost to restore the asset to a functional state. • Consider alternate solutions if less costly.	Direct damage and restoration > $1 billion	Direct damage and restoration $100 million to $1 billion	Direct damage and restoration $10 to $100 million	Direct damage and restoration $5 to $10 million	Direct damage and restoration $1 to $ $5 million	Direct damage and restoration under $1 million
Own Sector Impact • Estimate effect of loss of the asset on the sector in which asset resides (for example Transportation). • Consider redundancies, alternate suppliers if available.	Sector may shut down nationally or debilitating impact internationally	Debilitating impact on sector nationally	Debilitating impact on sector provincially or regionally	Debilitating impact on sector municipally **Or** Significant impact on sector provincially or regionally	Significant impact on sector municipally	Moderate impact on sector municipally
Other Sectors Impact • Estimate effect of loss of the asset on the other sectors (not the one in which asset resides). • Consider redundancies, alternate suppliers if available.	Debilitating impact on other sectors nationally	Debilitating impact on other sectors provincially or regionally	Debilitating impact on other sectors municipally **Or** Significant impact on other sectors provincially or regionally	Significant impact on other sectors municipally	Moderate impact on other sectors municipally	Minor impact on important missions of other sectors (municipally)
Recovery Time Impact • Estimate the time to restore the asset to a functional state. • Consider alternate solutions if time can be reduced (consistent with Recovery Cost Impact above).	Very long recovery time (longer than one year)	Long recovery time (months to 1 year)	Significant recovery time (weeks to 1 month)	Brief recovery time (days to 1 week)	Very Brief recovery time (hours to 1 day)	Minimal recovery time (minutes)
Public Confidence Impact	High National	Perceived high	Perceived high	Perceived high	Perceived	Perceived low

Impact Factor	Severe	Very High	High	Medium	Low	Very Low
Score	15	5	3	1	0.5	0.1
• Estimate the effect of the loss of the asset on public confidence in the ability of the relevant government to preserve public health and safety, economic security, or to assure the provision of essential services.	risk & ability to control in doubt	National risk & low ability to control risk **Or** High Provincial or Regional risk & ability to control in doubt	Provincial or Regional risk & low ability to control risk **Or** High Municipal risk & ability to control in doubt	Municipal risk & low ability to control risk	moderate Municipal risk & moderate ability to control risk	Municipal risk & high ability to control risk

Table 2. The Consequence of Loss Rating Table

DRDC has identified a number of problems with this rating methodology [47], which will be discussed in the following chapter.

4.2.3 Elicitation of Perspectives

The questions below were distributed to members of the BC CI Steering Committee for discussion at the January 2011 meeting. The purpose of the questions was to solicit feedback from the group on tools for the CIAP program.

- What of the asset assessment work completed to date is of continued value to asset owners?
- What challenges or problems have you encountered with any of the CI program tools? What changes to improve these tools can you offer?
- What is the value and purpose to a mathematical rating and / or ranking for every asset? How would this ranking be used?
- What information is needed to properly assess criticality?
- What information do asset owners want from the criticality assessment and what program areas could this be applied to?
- Moving forward, what information would asset owners be willing to share with the province?
- How would asset owners see participating in the evaluation of revised &/or new tools?

During the discussion, steering committee members stated that they wanted some sort of CI assessment tool. However, there was difficulty in articulating a clear purpose for such a tool.

During the second part of the interviews with EMBC regional staff from the six regions of BC (introduced in the HRVA section), a series of questions on CI were posed. The questions were as follows:

- What expectations do you have for a CI program in your region?

- What CI work has been done in your region, including by local authorities and other key stakeholders?
    - What were the results of the CI work?
    - What types of information do you and the local authorities currently have on critical assets/services within your regional office/PREOC?
    - What resources (information, tools, personnel, etc.) were used to attain this information?
- What has gone well with the CI work that has been done?
    - What do you like?
    - What do stakeholders like?
    - What would you like to continue to see?
- What would you like improved about the CI Program?
    - What would you like to be able to do as far as identification, data analysis and notification with critical infrastructure assets?
    - What additional resources would you like to have access to in order to support CI program in your region (information, qualified/knowledgeable personnel, tools, etc.)?
    - Have the local authorities in your region shared any thoughts or suggestions towards what they would like to see in place for a CI program?
- Additional Comments.

The need for a consistent approach throughout the province was recognized. However, CI awareness varied throughout the province with the southwest region of BC having focused on CI significantly more than any other region. Much of the exposure to CI in the province had come from the work that was done in marketing the CoL tool during the V2010 time frame.

4.2.4 Status of the EMBC CIAP

The CIAP was assessed by applying three complementary approaches for evaluating the requirements for a comprehensive CIAP and the gaps with current initiatives. These complementary approaches were:

- Systems engineering principles to assess the coherence, completeness, effectiveness and efficiency of requirements that were articulated in the CIAP or elicited from stakeholders; and to determine if these requirements were in a useable format that could direct further development and implementation of the CIAP by stakeholders;

- Capability based planning to assess the adequacy of current capabilities, in terms of people, processes, equipment and information, to conduct the key tasks, whether explicitly or implicitly, required for implementation of the CIAP by stakeholders; and

- Risk management principles (that is, ISO 31000) to determine how well the EMBC CIAP met international standards for "best practice" for risk management. See Annex A for more detail.

As mentioned previously, any successful public-private partnership requires a process for aligning the goals of various stakeholders. The importance of this challenge in any multi-agency initiative cannot be overstated, but addressing "goal alignment" is likely to be an on-going and iterative process. Therefore, while an assessment of gaps in a multi-stakeholder initiative like the EMBC CIAP using systems engineering, capability based planning and risk management as reference frameworks will be informative, it will likely also reveal the need for a process to address the underlying "wicked" problem to achieve an alignment of common goals across the stakeholder community and agreement on a collective action plan. Still, a number of gaps using the three complementary reference frameworks were identified with respect to the EMBC CIAP, and were grouped under the five categories of:

1. Planning;
2. Concepts;
3. Measurement;
4. Partnerships; and
5. Training.

Since the specific gaps include sensitive material, they are not included in this report. Details of the analysis and results are in the client letter report produced for EMBC [48].

5 Solution Identification and Evaluation

A key consideration in developing a solution strategy was the complex nature of the problem, which was reflected in the ambiguity in the overarching concepts or purposes of the EMBC programs. Action Research [48] has been developed as an exploratory and reflective approach to address complex issues. The principles articulated by Davison et al are:

- Development of an agreement that facilitates collaboration between the action researcher and the client;
- A cyclical model for research that consists of five stages: diagnosis, planning, intervention, evaluation and reflection;
- Understanding the critical role of theory as it relates to its implementation in practice;
- Change through action; and
- Learning through the implications of both research and practice.

The requirements and gaps assessment described in this report articulates the diagnosis stage of the research, while the solutions below describe potential interventions that might be implemented. The particular interventions were developed (in the planning stage) by considering the expertise and resources available to DRDC along with the EMBC gaps, and then consulting with EMBC executive and planning staff on which of the potential interventions would be chosen for implementation.

Of course, EMBC may undertake its own initiatives to address gaps identified in DRDC's client reports. The proposed projects in this chapter are not intended to preclude EMBC initiatives, but rather are intended to leverage DRDC expertise and partnerships.

The broad categories for the gaps identified as a result of the HRVA analysis are:

1. Risk management framework;
2. Regional HRVA;
3. Measurement and validation;
4. Partnerships; and
5. Training.

The categories of gaps identified as a result of the CI analysis are:

1. Planning;
2. Concepts;

3. Measurement;

4. Partnerships; and

5. Training.

Descriptions of the DRDC projects to address gaps in some of these areas are below.

5.1 Adaptation of Major Events Security Framework (MESF)

The Major Events Security Framework (MESF) [50] is a framework that has been developed by DRDC in conjunction with the RCMP with the vision of enhancing the preparedness of the Canadian Government through its security and safety stakeholders by formally establishing a standard and comprehensive approach to major event security and safety planning.

The development of the framework is based on the assumptions that current planning approaches do not provide for sufficient levels of information sharing and collaboration to achieve the necessary shared awareness and that collaborative planning allows all levels of government to plan together to synchronize their efforts. The proposed framework encompasses the following:

- Whole of government forum that guides the collaborative planning and execution of security capabilities;

- Knowledge management system that identifies best practices, captures lessons, effects change, and champions innovation;

- Repository of value-added tools and technologies; and

- Governance, with the authority to link policy, legislation and mandates with functions, tasks, and expertise, within the business planning cycle.

The current MESF runs on GCPEDIA, a federal government collaborative tool open to all federal employees. The MESF uses open source wiki software and can be easily and quickly adapted to meet the needs of the user community. For example a similar framework could be developed with EMBC to extend HRVA work in small communities and for CI planning. EMBC concept of operations document, plans, tools (for example, the HRVA Tool Kit, CI Spatial Query, etc.) and lessons learned could be used to populate an MESF-type framework.

5.2 Lessons and Tools from the Federal All Hazards Risk Assessment (AHRA)

Public Safety Canada's Federal All Hazards Risk Assessment (AHRA) was introduced in the literature review. A significant amount of work has been done by DRDC CSS in the development of the AHRA taxonomy, process, methodology and scoring, and scenario results. As a result of this work, DRDC has acquired expertise in the development and implementation of all hazards risk assessments. This knowledge can be used in the development of risk products for large

municipalities and/or regions and to aid in municipal risk mitigation planning (for example, though an extension of the HRVA Tool Kit to an HRVA risk management framework).

5.3 Scenario Mission to Task Templates

Scenarios can aid harmonized planning by providing a shared focus for stakeholders[17]. They help in the identification of an overarching shared risk treatment for the scenario - that is, the collective mission. The mission can subsequently be decomposed into key tasks described in enough detail that a given task could be undertaken by individual stakeholders with minimal direction. The process is sometimes referred to as a mission to task analysis.

This work is proposed to be undertaken through contract support. The intent of the contract is to develop hazard/scenario-based task templates to examine the utility of scenarios and mission to task analysis in supporting an effective holistic risk management framework for municipalities. This is proposed for one mid-size community (population 5000-50,000 and a volunteer fire department) and one large municipality (population > 50,000 and a professional fire department), with two scenarios per community[18]. The intent is to provide an urban case study in contrast to a mid-size community. The contractual tasks include: identifying the scenario missions and mission objectives; developing a measurement framework; identification of key tasks; synthesis of key tasks across scenarios; and evaluation of the utility of scenarios and mission-to-tasks analysis.

The specific municipalities will be determined in consultation with EMBC; however, the chosen communities should be ones that have already conducted a risk assessment using the HRVA Tool Kit or equivalent. The population of the two communities needs to be sufficiently distinct; for example, two communities of population (a) 10,000 and 60,000 or (b) 40,000 and 200,000 would provide a good range while two communities of population (c) 40,000 and 60,000 would not.

Mission to task analysis templates differ from those in the Target Capabilities List (TCL) mentioned in the CI literature search. The latter, the TCL, consist of tasks that are grouped functionally to facilitate the management of capabilities (that is, the development, deployment and sustainment of capabilities). Therefore, all tasks that are functionally similar (for example, all tasks related to a fire fighting capability) will be within the same TCL capability. The tasks in the mission to task templates are grouped according to all the tasks needed to achieve a desired effect or objective within a mission of a hazard or threat context even if the tasks are of a dissimilar functional nature (for example, to save lives in a given circumstance could conceivably require firefighting, police and emergency medical service tasks). If both the functional grouping of tasks within the TCL and the decomposition of the missions into required tasks are done well, it should be possible to map the mission tasks to the TCL tasks. This would enable a manager of

[17] A scenario here should be understood to be a set of shared assumptions around a particular hazard (for example, flooding from a particular water source). It should include full consideration of the many possible ways that flooding could occur and not be a particular and specific description of a future event. In other words, it is a framework for capturing the various assumptions each stakeholder explicitly or implicitly makes about the hazard.

[18] It should be noted that this is a feasibility study and not a full evaluation of the approach. Two scenarios for two communities were chosen to reduce the chance that the feasibility study was "lucky" in its selection of community and scenario. This is not intended to be a comprehensive evaluation, but it is consistent with participatory active research which takes an iterative approach to addressing complex issues.

a given capability to understand what is expected of his capability in the context of the given mission. Thus one long term aim of this work is to facilitate the coordination of capability management across the various agencies that would be involved in reducing risk from a given threat or hazard.

5.4 Community Resilience Framework

Architecture frameworks, such as the Department of National Defence and Canadian Forces Architecture Framework (DNDAF), in combination with operational research tools, such as soft systems methodology, are valuable in understanding the various perspectives of stakeholders, capturing the "as is" community system or system of systems, and identifying gaps in the shared awareness and understanding of the different stakeholders. Soft systems methodology aids this by providing a structured approach to capturing each stakeholder's perspective while architectural frameworks provide a structured way to collect information on the "as is" system and present that information in multiple ways through the various views supported by the architectural framework.

Recognising that communities, even small ones, are complex, interdependent systems, and that one member of the community can suffer a major disruption if other parts of the community are not prepared to respond to events, the UK has dedicated substantial resources to a project involving St Pancras Railway Station as a "community". The project applies architecture frameworks to create an understanding of the system and is looking at shared assessments of hazards and threats, a common framework for handling multi-stakeholder risks, and more effective and consistent risk mitigation strategies [51]. A similar approach is proposed here. While small and mid-sized communities have limited resources and might not have experience with architectural frameworks, they tend to have cohesive networks.

This work is proposed to be undertaken through contract support. The aim of the contract is to examine the utility of architectural frameworks and soft systems methodology in supporting a mid-size municipality (population 5000 to 50,000) in developing an effective holistic risk management framework for enhancing community resilience. The contract is intended to use only the most valuable elements of architectural frameworks, develop self-education tools, and provide online networking, wikis, etc. for shared support. The specific community will be determined in consultation with EMBC; however, the chosen community will be one that has already conducted an all hazards risk assessment using the HRVA tool kit or equivalent.

This work involves the integration of HRVA and CI work into an overarching risk management framework. This could help exploit the MESF work in terms of scaling the MESF concept for small municipalities.

5.5 Extensive Literature Searches

This report includes a high-level literature review for risk assessment and critical infrastructure, and literature searches have been performed for various other projects. Over time, the OR team has amassed a large base of reference material; however, extensive literature searches have not yet been documented. The intent is to hire a coop student to support the OR team in researching and documenting extensive literature searches for risk assessment and critical infrastructure for public safety and security, including recommendations for best practices. References are likely to

include the work of other nations, international standards, and academic and practitioner research. These literature searches will be used for education purposes both within CSS and externally, with best practices applied to various projects such as this and others.

5.6 Exploitation of Research on Multi-Agency Collaboration

The challenges associated with multiple agencies working together have been identified in numerous major events and disasters. Consequently, DRDC led a Technology Investment Fund (TIF) research program to better understand the psycho-social barriers to effective inter-agency collaboration and shared decision making. Under the research program, the University of Ottawa (UofO) developed a conceptual model of shared decision making or problem solving and tested the model through exercises involving emergency managers, first responders, military, and humanitarian aid workers [52]. The research found that:

- Coordination (that is, information sharing) is often used to solve complex problems that require deeper levels of collaboration (that is, shared agreement on the problem and goals and shared decision-making);
- Participants were more satisfied with outcomes and generated greater consensus-based decisions with collaboration compared to coordination; and
- Collaboration can be taught as a skill.

One lesson learned by EMBC from the V2010 experience was that multi-agency plans were often created as a result of challenges encountered in exercises, rather than before. The expertise developed by the UofO research team could be used to facilitate exercises that would help the CI community to identify shared goals and agree on an effective action plan to achieve those goals.

5.7 EMBC Consequence of Loss Tool (CoL) Development

The data collected using the EMBC Critical Infrastructure Identification and Rating Workbook for V2010 was provided to DRDC, as an agent of the Integrated Security Unit (ISU), for providing an analysis of CI for V2010. DRDC analysed data on more than 5000 assets that were evaluated by approximately 125 asset owner/operators using the rating workbook and its consequence of loss (CoL) assessment/rating methodology.

While the exercise of evaluating CI assets was very valuable and important information was collected, the analysis of the data led to the identification of issues with the CoL rating table [47], such as:

- An inconsistent mathematical framework:
    - The impact factors have both a verbal label (low to severe) and numeric (0.5-15) score, with an inconsistent scoring scale (increasing from lowest to highest by a factor of 5, 2, 3, 5/3, 3 for the numeric scores);

- The scales within impact factors are "mostly" logarithmic (increasing by a factor of 10) and pseudo-geometric (increasing by different factors within a category). Specifically, the population impact and recovery cost impact scales are mostly logarithmic; however, at the lower levels the ratios within the impact factors are not logarithmic. For example, for recovery cost impact from lowest to highest the scores increase by a factor of 5, 2, and then 10. The scale within the recovery time impact factor is pseudo-geometric going from minutes to hours to days to weeks to months to years. Furthermore, the overall scoring scale for impact factors is not consistent; that is, adjacent scores from very low to severe differ by a factor of 5, 2, 3, 5/3, and 3;

- Given the mix of scales, the degree of consequence across factors is inconsistent. For example, the equivalent dollar value of a human life is up to $250,000 for very low and low scores and $100,000 for medium to severe scores;

- The impact scores are summed for a final score, which is mathematically invalid. Since the scales are mostly logarithmic, adding scores does not obey the mathematical laws of logarithms;

- Correlated factors. Impact factors, in particular recovery cost, are not independent from recovery time. This leads to some degree of double counting;

- The mixes of public, asset owner, own sector, and other sector factors make it unclear as to what drives a high score and the significance of the score. An asset could be rated highly due to its value to the asset owner or to others (for example, an asset could have a high recovery cost and recovery time but have no value to others);

- Problems within impact factors:

    - Fatalities, injured, and evacuated people are considered to be equivalent (that is, 1 fatality = 1 injured = 1 evacuated), although this is not the case in reality;

    - The recovery cost does not reflect the economic cost to the community, only to the asset owner.

- Subjectivity in ratings. For V2010, the ratings were not validated. In some cases, different owners/operators scored the same assets significantly differently (for example, ATM machines). Asset owners also tended to overestimate the effects of their own sector on other sectors and on public confidence.

DRDC provided this feedback to EMBC [47] and has been working in conjunction with EMBC and the BC CI Steering Committee to develop an enhanced version of the assessment methodology. The proposed methodology distinguishes between impacts between different groups and considers consequences to assets owners, own and other CI sectors, and society separately. In particular, an enhanced tool should include a high-level, consequence to society framework that is based on the BC Emergency Response Management System (BCERMS) goals. This should aid with the integration of CI risk assessments with more general community wide HRVAs.

As mentioned previously, the CI community has had challenges with articulating the purpose of a CI assessment tool. In further discussions on the V2010 CoL tool, it was reported that the larger private sector companies used the tool to aid in discussions with the ISU and to validate already known CI issues; that is, asset owners know their assets and likely have their own assessment tools. However, for local authorities the tool provided a means to compile data on CI assets in one document. It is likely that local authorities don't have CI assessment tools and would benefit from a standard assessment tool to bring together multiple disciplines. To design a tool that meets user needs, we have to understand a number of factors, such as:

- The purpose of the tool;
- Questions the tool needs to answer;
- Decision-making processes.

To this end, further development would require collaboration with infrastructure owners. Therefore, we proposed CI pilot projects with the participation of one to two commercial companies from the transportation, energy, or communications sector, one urban local authority, and one rural local authority (potentially a regional district including rural local authorities). The intent is to work with specific companies/organizations to address high-priority CI issues that would likely be common to those in the CI community, and use the methodology and tools developed during the pilots to develop common tool(s) for the larger CI community. To date, TransLink has agreed to the pilot project as the commercial company, and the Corporation of Delta as the urban local authority.

It is important to note that a suite of tools may be required. One tool may not be able to answer all the questions of the CI community.

5.8 Adapting the V2010 Critical Infrastructure Asset Ordination (CIAO) Model

In order to assist the Integrated Security Unit with "the CI problem" for V2010, DRDC developed the Critical Infrastructure Asset Ordination (CIAO) model to identify CI areas that were the most critical to V2010 security operations. The CIAO model structured information into three layers: (1) high level risk factors related to overall games operations (for example, VIP security, economic disruption, host reputation, etc.), (2) functions required for a successful, safe and secure games (for example, theatre command, YVR airport, emergency response teams, etc.), and (3) the delivery of CI goods and services upon which those games functions were dependent (electricity, transportation, telecommunications, etc.). Each layer was related to the other layers through risk assessments.

The model captured subject matter expert assessments of the risk to games functions due to the loss or failure of CI services as well as the assessments of the risk to overall game operations due to the loss or failure of games functions. CI services were linked to CI assets through information provided by the CI asset owners and open source information. This allowed the ISU to trace the risk (likelihood and impact) associated with any given CI asset to the potential impact its loss could have on the overall games.

The output from the CIAO model, a list of prioritized CI services and assets, provided a means for the ISU to ”grasp” the CI problem and prioritize CI services and asset owners, facilitated discussions with key asset owners, shifted discussion from security personnel protection requests to coordinated response, and separated ISU CI issues from broader regional issues.

The CIAO model developed for the ISU can be adapted for use with other asset owners or across a community. At the asset owner/operator level, similarly to the approach taken with the ISU, the CIAO model could be used to identify key risk factors, business functions, and the CI services/assets they depend on. This would help in linking risk with CI services/assets and an improved understanding of the importance of CI services/assets to business operations. At the community level, the model could be used in a table top exercise based on a scenario built around a specific threat or hazard. This would help the CI community to better understand the risk associated with CI dependencies and to identify some of the key interdependencies amongst CI owners.

5.9 Adaptation of the UK’s Critical National Infrastructure (CNI) Approach

The United Kingdom has developed a framework and guidance for protecting their infrastructure, as outlined in the literature search. The framework includes a criticality scale that defines six categories of disruption or failure for essential services, from minor to catastrophic, for each of their nine CI sectors, and a threshold distinguishes critical national infrastructure from critical infrastructure. A similar approach could be used within BC to define criticality scales and critical “provincial” infrastructure. This could be incorporated with work on the CoL tool development, although would likely require the establishment of sector networks within the province in order to develop the criticality scales within each sector.

5.10 Adaptation of US CI Sector Information Reports

In collaboration with CI stakeholders, the Protective Security Coordination Division of the DHS Office of Infrastructure Protection has developed a series of information reports (for example, [53, 54, 55]) that describe:

- Each sector and its common vulnerabilities;
- Indicators and warnings for CI owners and operators to be aware of;
- Protective measures that should be taken at different levels of alert, and by whom; and
- Reference material and other useful information.

These information reports have been developed specifically for the prevention of terrorist actions against CI; however, the approach can be generalized and applied to any threat or hazard scenario and extended to all pillars of the emergency management cycle (mitigation/prevention, preparedness, response or recovery). Similar products could be developed for BC’s purposes through activities such as facilitated workshops and table top exercises.

5.11 Development of a Regional CI Systems of Systems Simulation

As introduced in the literature review, the University of British Columbia (UBC) has developed a dynamic computer simulation, i2sim, to model interaction amongst various CI systems. During V2010 DRDC contracted UBC to develop a model of the energy, communications, public safety, health, transportation, and water sectors in the downtown Vancouver area to assess the public safety effectiveness in evacuating casualties from BC Place following an earthquake. While the timing of the contract did not allow a full demonstration of the value of the i2sim simulation, i2sim could be used to:

- Identify vulnerabilities due to CI interdependencies;
- Validate response plans; and
- Serve as an event driver for exercises.

As part of the contract with UBC, DRDC CSS received copies of the i2sim software and has the in-house expertise to use it. To date i2sim has been based on modelling specific assets; however the systems dynamics approach is suitable for modelling function" (such as the function of delivering natural gas to a given region or municipality) instead of assets. This would allow the modelling of CI sector functions without representation of specific assets, which has been an area of concern for CI asset owners. The i2sim model could be applied to an area of interest to the CI community to model or represent the critical infrastructure functions in that area. Subsequently, the simulation could be used in a study to identify vulnerabilities or as an event driver for exercises.

5.12 Evaluation of Solutions

In the requirements and gaps letter reports provided to EMBC on HRVA [26] and CI [48], the potential of the above projects to address the various gaps was assessed as either significant, some, or considered to be minimal/nil, as shown in the tables below. Table 3 shows an assessment for the projects relative to the gaps of the HRVA program.

	Gaps				
DRDC Proposal	**Risk Management Framework**	**Regional HRVA**	**Measurement and Validation**	**Partnerships**	**Training**
P1. MESF	Significant	Significant	Some	Significant	Significant
P2. AHRA	Some	Significant	Significant	Significant	
P3. Template	Significant	Some	Some	Some	Some
P4. Resilience	Significant	Some	Some	Significant	Some
P5. Literature	Significant	Some	Significant		Some
P6. Collaboration	Significant	Significant		Significant	Significant

Table 3. DRDC Proposal Potential to Address HRVA Program Gaps

Note that all of the projects have the potential to address gaps in multiple categories to some degree, while projects such as Adaptation of the MESF (P1) and Exploitation of Research on Multi-Agency Collaboration (P6) have significant potential to address gaps in most categories.

Table 4 gives an assessment for the proposals relative to the gaps of the CIAP.

	Gaps				
DRDC Proposal	**Planning**	**Concepts**	**Measurement**	**Partnerships**	**Training**
P1. MESF	Significant	Some		Significant	Significant
P2. AHRA	Some		Significant	Some	
P3. Template	Significant	Significant	Some	Some	Some
P4. Resilience	Significant	Significant	Some	Significant	Some
P5. Literature	Some	Some	Significant		Some
P6. Collaboration	Significant	Significant		Significant	Significant
P7. CoL Tool	Some		Significant		
P8. CIAO	Some	Some	Significant	Some	
P9. UK CPNI	Some	Some	Significant		Some
P10. DHS	Significant	Some		Significant	Significant
P11. i2sim	Some	Some	Significant	Some	Significant

Table 4. DRDC Proposal Potential to Address CI Program Gaps

Again, all of the proposed projects have the potential to address multiple gaps to some degree. However, the Exploitation of Research on Multi-Agency Collaboration (P6) has significant potential to address gaps in most categories.

In addition, the following table was presented to demonstrate that there might be extra value in undertaking several related DRDC proposals. In the table an "X" at the intersection of two proposals indicates the potential for some additional benefit (for example, there would be better results from at least one of the proposals) associated with undertaking those two proposals ("n/a" for "not applicable" is used for the intersection of a proposal with itself).

	DRDC Proposal										
DRDC Proposal	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**
P1. MESF	n/a	X	X	X	X	X	X	X	X	X	X
P2. AHRA	X	n/a			X		X	X	X		
P3. Template	X		n/a	X		X		X	X	X	X
P4. Resilience	X		X	n/a		X		X	X	X	X
P5. Literature	X	X			n/a		X	X			X
P6. Collaboration	X		X	X		n/a	X	X	X	X	X
P7. CoL Tool	X	X			X	X	n/a		X		
P8. CIAO	X	X	X	X	X	X		n/a	X	X	X
P9. UK CPNI	X	X	X	X		X	X	X	n/a		X
P10. DHS	X		X	X		X		X		n/a	X
P11. i2sim	X		X	X	X	X		X	X	X	n/a

Table 5. DRDC Proposal Intersection

As viewed in the table, all projects overlap with others to some degree. However, Adaptation of the MESF (P1) project intersects with every other project.

The results of the requirements and gaps analysis for CI and the proposed DRDC projects were presented to the BC CI Steering Committee on September 29, 2011, and the results for both HRVA and CI and the proposed projects were presented to the EMBC Executive and Integrated Planning team on October 25, 2011. The work on CI assessment methodologies and tools was viewed as a high priority given the issues with the CoL tool and the need for tools in the user community. Adaptation of the MESF work was regarded very positively and would meet the needs of some of the current projects of the Integrated Planning business unit. There was also a lot of interest in the multi-agency collaboration work. However, it was agreed that the latter two proposals would be better pursued at a later date once some of the groundwork had been laid through other projects, especially given the high resource requirements. General support was given for the remaining projects.

Towards the end of the discussion, the projects were grouped into four categories, and the summary matrix in the table below was prepared for EMBC. Note that the table does not include the literature search, which is intended for completion, or the multi-agency collaboration work, since funding has not yet been approved. Projects seven through nine are grouped under “CI Assessment Tools”.

Project Details			Resources		
Title	**Objective**	**Approach**	**DRDC**	**EMBC**	**Community/Agency Engagement**
Event Planning Framework	Provide an internet, wiki-based collaborative environment	Exploit similar DRDC work (Major Events Security Framework) done in support of the RCMP Protective Policing Branch	1-2 Person Months	Participation in a workshop to define requirements	None
Community Resilience Framework[19]	Provide a guide to assist the EPC of a mid-sized community with the harmonization of individual community member risk management plans	Exploit UK work on improving community resilience through the application of architectural frameworks	Contract: $200K,; Duration : 1 year from award of contract[20]	Selection of communities; Project Oversight	Participation of a mid-size community[21] (population 5k-50k) which has conducted an all hazards risk assessment
Mission to Task Template[22]	Provide a task template that assists EPC with the development of a hazard specific community wide plan as well as a framework for assessing the effectiveness of community measures related to a specific hazard	Use a top down approach (mission to tasks) to identify the concept of operations, objectives and key tasks needed to address a specific hazard	Contract: $200K Duration: 1 year from award of contract[23]	Selection of communities; Project Oversight	Participation of a mid size community[24] (pop 5k-50k volunteer fire dept) and a large community[25] (>50K, professional fire dept); both communities should have conducted an all hazards risk assessment
CI Assessment Tools	Develop value-added tools for CI asset owners	Identify tool requirements through direct work with CI asset owners; exploit work done by EMBC and DRDC for V2010 as well as similar work done by the UK	1.5 Person Years	Project Oversight and part of the development team – develop, test, validate	Participation of 1-2 commercial companies, 1 urban local authority, 1 rural local authority (perhaps a regional district including rural LAs)

Table 6: EMBC-DRDC Projects Related to HRVA and CI Assurance Programs

[19] Where appropriate, this work will be coordinated with the CRTI funded project involving JIBC and Royal Roads.
[20] Date of contract award is estimated to be sometime in the first half of 2012.
[21] Mid-sized community: These requirements are not rigid. The intent is to focus on communities with limited resources, especially limited full-time / professional resources. While the community should be large enough so that a structured approach is worthwhile, it should be small enough that the various stakeholders are well known to each other. There is a slight preference to the lower end of the population range.
[22] Where appropriate, this work will be coordinated with the CRTI funded project involving JIBC and Royal Roads.
[23] Date of contract award is estimated to be sometime in the first half of 2012.
[24] Mid-sized community: The requirements are similar to the "mid-sized" community for the "community resilience framework", but there is a slight preference to the higher end of the population range.
[25] Large community: The intent is to provide an urban case study in contrast to the mid-sized community. Therefore, the selection of both communities needs to be considered together. For example, two communities of 10K and 60K or two communities of 40K and 200K provide a good range while two communities of 40K and 60K would not

6 Summary

EMBC and DRDC entered into a collaborative project agreement following Vancouver 2010. This paper presented the problem formulation and solution strategy work that was completed as the first phase of the collaborative project, examining EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Assurance programs. The document discussed the methodology, presented literature searches on risk assessment and critical infrastructure, provided high level information regarding the analysis and status of EMBC's programs, and identified and evaluated solutions.

The current objectives associated with the EMBC HRVA and CI Assurance programs along with their multi-agency aspects lead them to fall under the category of wicked problems, which means, among other things, that the problem can be viewed differently (and legitimately) from different stakeholders' perspectives . The foundation of the DRDC approach was the NATO Code of Best Practice for C2 Assessment, using soft operations research to address the initial problem formulation (which is likely to be iterative). This included engaging various stakeholders to elicit their perspectives, and using this information to formulate the problem.

Performing an analysis using aspects of capability based planning, systems engineering and risk management principles, the requirements for and gaps in the EMBC programs were identified. A number of projects were proposed by DRDC to address aspects of the gaps, which are currently at various stages:

- TransLink and the Corporation of Delta have been engaged for pilot projects for the development of CI assessment methodologies and tools, and a rural regional district has been identified but not yet approached;
- Contracts for the scenario mission to task analysis/templates and the community resilience framework were posted on Merx to advertise for requests for proposals and the resulting bids evaluated;
- A co-op student has been chosen to work on extensive literature searches;
- The province is exploring access to GCPEDIA in order to pursue work related to the Major Events Security Framework; and
- The University of Ottawa has been engaged in discussions on potential follow-on work on multi-agency collaboration.

Formulating or framing a complex problem such as identifying an agreed way forward for each of the two EMBC programs is neither easy nor a short term task. It is an on-going task. The above projects were proposed, in part, to address some of the more readily identified gaps but also, in part, to further the problem formulation process. The ultimate goal of this work is shared awareness among EMBC and the community stakeholders, along with an agreed action plan that includes the development of appropriate methodologies, tools, and information to benefit the Canadian public safety and security community.

References

[1] *Emergency Management BC – DRDC Centre for Security Science Collaborative Work Plan*, 7 March 2011

[2] Genik, L., Smith, D., *Command and Control Analysis of the South West Provincial Regional Emergency Operations Centre during Vancouver 2010*, 16th ICCRTS, June 1, 2011

[3] *Emergency Management in BC: Reference Manual*, Emergency Management British Columbia, August 2011, 171 pages, available from http://www.pep.bc.ca/training/reference_manual.pdf

[4] *NATO Code of Best Practice for C2 Assessment*, Command and Control Research Program, Department of Defence, 2002.

[5]] *NATO Handbook on Long Term Defence Planning*, RTO-TR-69, NATO Research and Technology Organization, 2003

[6] Hales, D., Chouinard, P., *Implementing Capability Based Planning within the Public Safety and Security Sector Lessons from the Defence Experience*. DRDC CSS Technical Memorandum DRDC CSS TM 2011-26, December 2011, 88 pages

[7] Davis, P., *Analytical Architectures for Capabilities-Based Planning, Mission-System Analysis and Transformation*, MR-1513, Rand, 2002.

[8] *Guide to Capability Based Planning*, The Technical Cooperation Program, Joint Systems and Analysis Group, Technical Panel 3, 2004.

[9] Rittel, H.W.J., and Webber, M. M., *Dilemmas in a General Theory of Planning*, Policy Sciences 4 (1973), p. 155-169.

[10] Checkland, P. and Holwell, S., *"Classic" OR and "Soft" OR – an Asymmetric Complementarity*, in Systems Modelling: Theory and Practice, Edited by M. Pidd, John Wiley & Sons, 2004.

[11] Pate-Cornell, M. E., *Uncertainties in risk analysis: Six levels of treatment, Reliability Engineering and System Safety*, 54 (1996) pp 95-111

[12] *Risk Management – Principles and Guidelines on Implementation*. International Organization for Standardization ISO 31000, 2009, First Edition

[13] Committee to Review the Department of Homeland Security's Approach to Risk Analysis; National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, The National Academies Press, 2010, 160 pages, available from http://www.nap.edu/catalog.php?record_id=12972

[14] Cox, L.A., *What's Wrong with Risk Matrices?*, Risk Analysis, Vol 28, No 2, 2008, pp. 497-512

[15] Hubbard, D., Evans, D., *Problems with Scoring Methods and Ordinal Scales in Risk Assessment*, IBM Journal of Research and Development, Vol 54, No 3, Paper 2, May/June 2010, pp. 2:1-2:10

[16] Pruyt, E., Wijnmalen, D., *National Risk Assessment in the Netherlands A Multi-Criteria Decision Analysis Approach*. Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems , Lecture Notes in Economics and Mathematical Systems, 2010, Volume 634, Part 2, pp. 133-143

[17] *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands*, October 2009

[18] UK Cabinet Office, *National Risk Register of Civil Emergencies 2010 edition*, 2010

[19] *Guide to Integrated Risk Management*, Treasury Board Secretariat, available from http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirpr-eng.asp?format=print

[20] *Framework for the Management of Risk*, Treasury Board Secretariat, available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text

[21] *All Hazards Risk Assessment Methodology Guidelines 2011-2012*, Public Safety Canada, December 2011

[22] *BC Emergency Program Act*. [RSBC 1996] Chapter 111. Available from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_96111_01

[23] *British Columbia Hazard, Risk and Vulnerability Analysis Tool Kit*. Ministry of Public Safety and Solicitor General, Provincial Emergency Program, 2004

[24] Paul Chouinard, email to Heather Lyle *"Quick Look at EMBC HRVA",* February 2, 2011

[25] *EMBC Strategic Planning, Policy and Legislation Organisational Chart and Key Project Areas*, August 4, 2010

[26] Genik, L., Chouinard, P., *Hazard Risk and Vulnerability Analysis in BC: Requirements and Gap Assessment and DRDC Proposals for Support*, DRDC Letter Report to EMBC, September 14, 2011, File 3700-1

[27] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, United States, February 2003, available from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[28] *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, Department of Homeland Security, 2009, 188 pages, available from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf,

[29] *Critical Infrastructure Resilience: Final Report and Recommendations*, US National Infrastructure Advisory Council, 8 Sept 2009, 54 pages

[30] *National Incident Management System*, Department of Homeland Security, March 1, 2004, 130 pages

[31] *National Preparedness Guidelines*, Department of Homeland Security, September 2007, 51 pages, available from http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf

[32] *Target Capabilities List*, Department of Homeland Security, September 2007, 588 pages

[33] *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, UK Cabinet Office, March 2010

[34] *CNI Protection in the United Kingdom. Framework and Guidance*, Centre for the Protection of National Infrastructure, September 2008

[35] *CNI Protection in the United Kingdom Framework and Guidance: Annexes*, Centre for the Protection of National Infrastructure, September 2008, 17 pages, UK Restricted

[36] *National Strategy for Critical Infrastructure Protection*, Federal Ministry of the Interior, Federal Republic of Germany, 17 June 2009, 18 pages

[37] *National Strategy for Critical Infrastructure*, Federal, Provincial and Territorial Governments of Canada, 2009

[38] *Action Plan for Critical Infrastructure*, Federal, Provincial and Territorial Governments of Canada, 2009, 25 pages

[39] *Canada-United States Action Plan for Critical Infrastructure*, Department of Homeland Security and Public Safety Canada, 2010, 9 pages

[40] A number of i2Sim publications are available from: http://www.ece.ubc.ca/~jiirp/publications.html

[41] Robert, B., Morabito, L.and Quenneville, O. (2007) *The Preventive Approach to Risks Related to Interdependent Infrastructures*, Int. J. Emergency Management, Vol. 4, No. pp.166–182

[42] Goldsmith, S., Eggers, W.D., *Governing by Network: The New Shape of the Public Sector*, Brookings Institution Press, December 2004, 224 pages, ISBN-10: 0815731280

[43] Myles, M., Lyle, H., *Critical Infrastructure Assurance Program: Concept Paper*, draft, Emergency Management British Columbia, October 2010.

[44] *Critical Infrastructure Identification & Rating Workbook The 2010 Games Critical Infrastructure Initiative*, EMBC, April 24, 2008 version 2, 48 pages

[45] *IPREM Strategic Plan 2011-2012*, available from http://www.metrovancouver.org/IPREM/IPREMDocs/IPREMStrategicPlan2011-2012.pdf

[46] *Critical Infrastructure Rating Workbook*, Provincial Emergency Program, EMBC, May 2007 Freshet Pilot version 2, 37 pages, http://www.pep.bc.ca/community/CI-RatingsWkbk.pdf

[47] Chouinard, P., *Feedback on the JELC Data Collection Sheet*, 3782-2008-33bd (PM MECSS), 13 May 2009

[48] Davison, R., Martinsons, M.G., Kock, N., *Principles of Canonical Action Research, Information Systems Journal*, Vol. 14, Issue 1, January 2004, pp. 65-68

[49] Chouinard, P., Genik, L., *The Resiliency of BC's Critical Infrastructure Requirements and Gaps Assessment and DRDC Options for Support*, DRDC Letter Report to EMBC, September 14, 2011, File 3700-1

[50] *Major Events Security Framework Strategic Vision*, 2011, available from http://www.gcpedia.gc.ca/wiki/MESF/About/Strategic_Vision_of_MESF

[51] Osborn, C., Marzell, L., *UK experience - Study of St. Pancras Railway Station*. Presented at the DRDC CSS Summer Symposium, June 15, 2010

[52] Lemyre, L. et al, *Research Using In Vivo Simulation of Meta-Organizational Shared Decision-Making (SDM),* DRDC CORA TR [W7714-083659/001/SV], August 2011

[53] *Characteristics and Common Vulnerabilities Infrastructure Category: Dams*, Protective Security Coordination Division, Office of Infrastructure Protection, US DHS, 5 Oct 2007, For Official Use Only

[54] *Potential Indicators of Terrorist Activity Infrastructure Category: Dams*, Protective Security Coordination Division, Office of Infrastructure Protection, US DHS, 5 Oct 2007, For Official Use Only

[55] *Protective Measures Infrastructure Category: Dams*, Protective Security Coordination Division, Office of Infrastructure Protection, US DHS, 5 Oct 2007, For Official Use Only

[56] Journeay, M., *Disaster Resilience by Design: A Framework for Integrated Assessment and Risk-Based Planning in Canada*. Natural Resources Canada and the Canadian Institute for Partners, June 2011, 336 pages

Annex A ISO 31000 Principles Applied to CI

Enhancing the resiliency of critical infrastructure can be seen as a form of risk management. Therefore the principles of ISO 31000 [ISO] discussed previously should apply to a critical infrastructure program. However, one issue not discussed in ISO 31000 is that the risks due to CI vulnerabilities are borne by the whole of society and all elements of society (government, the private and voluntary sectors and even individuals) have some responsibility to manage CI related risks. While applying ISO 31000 to the risks faced by a single enterprise can be challenging, applying the principles to a societal wide or any multi-enterprise risk management process adds a whole new level of complexity. Using the framework of the ISO principles, questions were identified that related to the challenge of applying those principles to the multi-agency context of the enhancing the resilience of CI. The EMBC CIAP was then evaluated to determine if these questions were addressed and whether or not solutions were provided. The effectiveness of the solutions was not evaluated. The questions considered, listed by the ISO 31000 principles, are as follows:

a) Creates and protects value: Whose value? What if the value created or protected is only for some agencies but the costs are borne by others? What if there is not agreement on the values to be created or protected? For example, private enterprises legitimately, may be more concerned about their profits, while governments will be concerned about general societal values. Can there still be collaboration amongst the various agencies when there is no overlap in values? What does the community do about “free riders”, that is, those who benefit from the investments of other members of the community? What about the ‘tragedy of the commons” where no one takes responsibility for protecting something of value to everyone but there is no clearly identified responsible agency?

b) Integral part of all organizational processes: Ideally all agencies would have CI risk management as a part of the organizational processes. Practically that will not happen. There will be different levels of integration from not at all to an extensively integrated process. A practical CI program must account for varying degrees of integration as well as actively promote good practices amongst all agencies.

c) Part of decision making: Different agencies will have decision making processes that vary in terms of sophistication, issues other than CI risk that must be addressed, and so on. How will these varying decision making processes be coordinated to ensure that risk is reduced or that new risks are not introduced? It’s worth noting that CI asset owners that are competitors will not want to divulge their decisions to each other and coordination in this circumstance may be very limited in scope.

d) Explicitly addresses uncertainty: Managing risk across multiple agencies introduces new uncertainties since there will be incomplete information on the extent to which other agencies are addressing risk. Any agency’s plans will to some degree depend on other agencies. Each such dependency introduces uncertainty if the agency does not confirm their assumptions. While agencies can explicitly identify those assumptions how will they address those assumptions and the uncertainty that those agencies upon whom they depend will act in the way they assume?

e) Systematic, structured and timely: As has already been discussed it must be accepted that the implementation of risk management will vary across agencies so it can be expected that there will be varying degrees of how systematic or structured the risk management processes are across the various agencies. The question of timeliness causes another element of discord since some agencies, such as those in high technology are communications, are in highly dynamic industries with very short long-term horizons (for example, measured in months) while others, such as those in capital intensive utilities, have more deliberate investment processes that require a longer process that is in some cases measured in years (for example, the building of dam).

f) Based on the best available information: There will be to some extent a disparity of information across the various agencies and the fact that some information is proprietary will mean that any given agency will not have the best information available. In some cases they may not even know if the information is available or not. Other agencies that might have the required information may not know that they do or may not be willing to divulge the information. How will an effective CI program facilitate the identification of information that should be shared and ensure that it is properly handled once shared?

g) Tailored: Tailoring a risk management process across the various multiple agencies is a daunting task. What elements should be common to all agencies or groups of agencies? Which elements should be left to each individual agency? Organizing the agencies into "sectors" is one way to manage the complexity associated the varying needs of each agency, but any organizing principle has limited validity and could introduce an additional barrier to coordination. How will a CI program mitigate against barriers associated with organizing agencies into "sectors".

h) Takes human and cultural factors into account: There is little doubt that a societal wide program to address CI risk must take human and cultural factors into account, but how? Key elements will include building trusted relationships and ensuring a common understanding across the community.

i) Transparent and inclusive: Since CI risks are faced by all of society, even if CI program does not include all agencies in the explicit risk management process, and, indeed, cannot realistically include all agencies, there must still be an "outreach" element of the process that allows those agencies that are not active members to make informed decisions with respect to CI related risks. Not doing so unnecessarily increases risk. Does the CI program include an effective "outreach element"? Can this be balanced with the legitimate desire of the active members of the CI to protect proprietary information?

j) Dynamic, iterative and responsive to change: The requirement to be dynamic, iterative and responsive to change will vary across the various agencies involved with managing CI related risks due to the varying characteristics and circumstances of each agency. As each agency responds to its dynamic needs and changing circumstances what will be the implications for other agencies? Will they even be aware of changes that may affect their own risk management processes and plans? As well, the iterative application of risk management will vary across agencies. As a result one-time, validated assumptions other agencies may have with respect to with a given agency might have changed as a result of asynchronous iterations of risk management across the community. How will changes introduced to iterative changes on different cycles across the community be synchronized?

k) Facilitates continual improvement of the organization: While there are well-known challenges to a becoming a “learning organization”, there are demonstrated best practices. How can these best practices be implemented in a distributed risk management process that is required by an effective CI program? Are these practices even still valid for a risk management process distributed across multiple agencies?

The questions articulated are by no means comprehensive but they are illustrative of the various issues that an effective CI program must explicitly address. These issues arise from difficulty in defining the scope of a risk management process when that process is distributed across multiple agencies. While defining a scope is necessary to make the process manageable, care must be taken that the, to some degree, artificially defined scope does not introduce additional, unacceptably high risks. A CI program that assumes the challenges with addressing the above questions do not exist could be unconsciously introducing additional risks as has been demonstrated on past events where failure and disaster have occurred due to organizations failing to collaborate, cooperate and coordinate adequately.

List of symbols/abbreviations/acronyms/initialisms

ACAMS	Automated Critical Asset Management System
ADM	Assistant Deputy Minister
AHRA	All Hazards Risk Assessment
BC	British Columbia
BCERMS	British Columbia Emergency Response Management System
BMAP	Bomb-Making Materials Awareness Program
BTRA	Biological Threat Risk Assessment
C2	Command and Control
CBP	Capability Based Planning
CI	Critical Infrastructure
CIAO	Critical Infrastructure Asset Ordination
CIAP	Critical Infrastructure Assurance Program
CI/KR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
CISQ	Critical Infrastructure Spatial Query
CNI	Critical National Infrastructure
CoL	Consequence of Loss
CPNI	Centre for the Protection of National Infrastructure
CSS	Centre for Security Science
DHS	Department of Homeland Security
DRDC	Defence Research and Development Canada
EM	Emergency Management
EMBC	Emergency Management British Columbia
EMC	Emergency Management Committee
EPA	Emergency Program Act
FEMA	Federal Emergency Management Agency
HRVA	Hazard Risk Vulnerability Analysis/Assessment
i2Sim	Infrastructure Interdependencies Simulation
ICS	Incident Command System
IPREM	Integrated Partnership for Regional Emergency Management

IPS	Integrated Public Safety
ISO	International Standards Organization
ISU	Integrated Security Unit
JIBC	Justice Institute of British Columbia
LA	Local Authority
MCDA	Multi-Decision Criteria Analysis
MECSS	Major Events Coordinated Security Solutions
MESF	Major Events Security Framework
NATO	North American Treaty Organization
NDA	Non-Disclosure Agreement
NIMS	National Incident Management Standard
NIPP	National Infrastructure Protection Plan
NRA	National Risk Assessment
OR&A	Operations Research and Analysis
PCII	Protected Critical Infrastructure Information
PECC	Provincial Emergency Coordination Centre
PREOC	Provincial Regional Emergency Operations Centre
PSC	Public Safety Canada
R&D	Research and Development
RA	Risk Assessment
RCMP	Royal Canadian Mounted Police
RM	Regional Manager
S&T	Science and Technology
SME	Subject Matter Expert
SSA	Sector-Specific Agencies
TBS	Treasury Board Secretariat
TCL	Target Capabilities List
TIF	Technology Investment Fund
TRAM	Terrorism Risk Assessment and Management
TTCP	The Technical Cooperation Program
UofO	University of Ottawa
UBC	University of British Columbia

UK	United Kingdom
US	United States
V2010	Vancouver 2010 Olympic and Paralympic Winter Games
VIP	Very Important Person

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, for example Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Centre for Security Science (CRTI/PSTP)
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
NON-CONTROLLED GOODS
DMC A
Review: ECL June 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Genik, L., Chouinard, P.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2012	65	56

7. DESCRIPTIVE NOTES (The category of the document, for example technical report, technical note or memorandum. If appropriate, enter the type of report, for example interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science (CRTI/PSTP)
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
File 3700-1	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TM 2012-015	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unclassified

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This paper presents the problem formulation and solution strategy component of the EMBC-DRDC collaborative project agreement for improving EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Assurance Programs. The methodology is described; the NATO Code of Best Practice for C2 Assessment and a soft operations research approach were applied, along with aspects of capability based planning, systems engineering, and risk management. Preliminary literature searches were performed and are documented here. Stakeholder groups are described and the questions used to elicit their perspectives on the programs and related issues are presented. The result of the analysis was the identification of program requirements, gaps, and proposed projects by DRDC to address aspects of the gaps. The proposed projects include adapting the Major Events Security Framework for use by EMBC, CI assessment tool development through pilot projects, and contracts for a community resilience framework and scenario mission to task templates, among several others.

Le présent rapport explique les stratégies de formulation et de résolution du problème du projet collaboratif de RDDC et d'EMBC visant à améliorer les programmes d'analyse des dangers, des risques et de la vulnérabilité (ADRV) et d'infrastructures essentielles (IE). On y décrit la méthodologie employée, qui se résume à ceci : utilisation d'une approche de recherche opérationnelle souple et application des principes du Code des pratiques exemplaires d'évaluation du C2 de l'OTAN à divers aspects de la planification axée sur les capacités, à l'ingénierie des systèmes et à la gestion des risques. Les recherches documentaires préliminaires sont aussi décrites dans le présent rapport. On y présente les groupes d'intervenants consultés et les questions qui leur ont été posées afin de recueillir leurs points de vue au sujet des programmes à l'étude et des problèmes connexes. L'analyse a permis de cerner les besoins et les lacunes des programmes et de proposer des projets de RDDC en vue de combler les lacunes en question. Parmi ces propositions, on trouve notamment l'adaptation du Cadre de sécurité des grands événements pour les besoins d'EMBC, le développement d'un outil d'évaluation des infrastructures essentielles dans le cadre de divers projets pilotes, et l'octroi de contrats pour l'établissement d'un cadre de résilience communautaire et l'élaboration de modèles de synthèse mission-tâches.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, for example Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Critical Infrastructure (CI); Hazard Risk Vulnerability Analysis (HRVA); Risk Assessment; Soft Systems Methodology; Soft Operational Research and Analysis; Wicked Problems; NATO Code of Best Practice for C2 Assessment; Emergency Management British Columbia